101665,484

6

# 日 本 国 特 許 庁
# JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２００３年 ９月 ５日

出 願 番 号
Application Number: 特願２００３－３１４４６４

[ST. 10/C]: [ＪＰ２００３－３１４４６４]

出 願 人
Applicant(s): 株式会社リコー

２００３年１０月 ７日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号 出証特２００３－３０８２７２６

【書類名】　特許願
【整理番号】　0304084
【提出日】　平成15年 9月 5日
【あて先】　特許庁長官　今井　康夫　殿
【国際特許分類】　G06F 12/00　537
【発明者】
　【住所又は居所】　東京都大田区中馬込１丁目３番６号　株式会社リコー内
　【氏名】　斉藤　敦久
【発明者】
　【住所又は居所】　東京都大田区中馬込１丁目３番６号　株式会社リコー内
　【氏名】　金井　洋一
【発明者】
　【住所又は居所】　東京都大田区中馬込１丁目３番６号　株式会社リコー内
　【氏名】　谷内田　益義
【特許出願人】
　【識別番号】　000006747
　【氏名又は名称】　株式会社リコー
【代理人】
　【識別番号】　100070150
　【弁理士】
　【氏名又は名称】　伊東　忠彦
【先の出願に基づく優先権主張】
　【出願番号】　特願2002-273985
　【出願日】　平成14年 9月19日
【先の出願に基づく優先権主張】
　【出願番号】　特願2002-275973
　【出願日】　平成14年 9月20日
【先の出願に基づく優先権主張】
　【出願番号】　特願2002-297888
　【出願日】　平成14年10月10日
【手数料の表示】
　【予納台帳番号】　002989
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9911477

【書類名】特許請求の範囲
【請求項１】
ドキュメントの識別情報を読み取る識別情報読取手段と、
上記識別情報によって指定される動作要件を選択する動作要件選択手段と、
上記動作要件選択手段によって選択された１つ以上の動作要件に従って所定動作の実行を制御する動作制御手段とを有することを特徴とする画像形成装置。
【請求項２】
前記動作要件は、上記ドキュメントに対するセキュリティに関する要件であることを特徴とする請求項１記載の画像形成装置。
【請求項３】
上記所定動作は、電子データで画像を形成することを特徴とする請求項１又は２記載の画像形成装置。
【請求項４】
上記所定動作は、上記ドキュメントを用紙上に印刷することを特徴とする請求項１又は２記載の画像形成装置。
【請求項５】
上記識別情報読取手段は、
上記ドキュメントに対する所定読み取り動作によって取得したデータを上記識別情報として認識する識別情報認識手段と、
上記識別情報とドキュメント属性とを対応付けして管理するドキュメント属性管理手段と、
ドキュメント属性管理手段を参照することによって、上記識別情報認識手段よって認識された上記識別情報に対応する上記ドキュメント属性を取得するドキュメント属性取得手段とを有することを特徴とする請求項１乃至４のいずれか一項記載の画像形成装置。
【請求項６】
上記所定読み取り動作は、上記ドキュメントが用紙である場合に、該ドキュメントに印字されたバーコード、二次元コード又は磁気コード、又は、該ドキュメントに付与されたＲＦＩＤのいずれかを読み取って上記識別情報として認識することを特徴とする請求項５記載の画像形成装置。
【請求項７】
上記所定読み取り動作は、上記ドキュメントが用紙である場合に、該ドキュメントを読み取って生成される電子画像データから、バーコード、二次元コード、数字情報、文字情報、ドットパターンのいずれかを上記識別情報として認識することを特徴とする請求項５記載の画像形成装置。
【請求項８】
上記所定動作を要求するユーザに関するユーザ属性を取得するユーザ属性取得手段を更に有することを特徴とする請求項１乃至７のいずれか一項記載の画像形成装置。
【請求項９】
上記ユーザ属性取得手段は、
上記ユーザから該ユーザを識別するユーザ識別情報を取得するユーザ識別情報取得手段と、
該ユーザ識別情報と上記ユーザ属性とを対応付けして管理するユーザ属性管理手段と、
上記ユーザ識別情報に基づいて上記ユーザを認証するユーザ認証手段と、
上記ユーザ認証手段による認証結果に基づいて、上記ユーザ属性管理手段を参照することによって、上記ユーザ識別情報取得手段によって取得された上記ユーザ識別情報に対応する上記ユーザ属性を取得するユーザ属性取得手段とを有することを特徴とする請求項８記載の画像形成装置。
【請求項１０】
上記ユーザ属性取得手段は、
上記ユーザから該ユーザを識別するユーザ識別情報を取得するユーザ識別情報取得手段

と、
　上記ユーザを認証し、上記ユーザ属性を提供する外部サーバに対して該ユーザ属性を要求するユーザ属性要求手段とを有することを特徴とする請求項８記載の画像形成装置。
【請求項１１】
　上記動作要件が実行可能であるか否かを判断する動作要件判断手段と、
　上記動作要件判断手段による判断結果が上記動作要件が実行可能でないことを示す場合、上記所定動作を禁止する動作禁止手段とを有することを特徴とする請求項１乃至１０のいずれか一項記載の画像形成装置。
【請求項１２】
　上記動作要件は、上記ドキュメント対する上記所定動作の実行の際に、電子透かしを埋め込むことを指示することを特徴とする請求項１乃至１１のいずれか一項記載の画像形成装置。
【請求項１３】
　上記動作要件は、上記ドキュメント対する上記所定動作の実行の際に、表示可能なラベルを埋め込むことを指示することを特徴とする請求項１乃至１１のいずれか一項記載の画像形成装置。
【請求項１４】
上記表示可能なラベルは、少なくとも上記所定動作を要求したユーザの認証データと、上記所定動作を要求した時点のタイムスタンプを含むことを特徴とする請求項９乃至１１のいずれか一項記載の画像形成装置。
【請求項１５】
　上記動作要件は、上記ドキュメント対する上記所定動作の実行の際に、少なくとも上記所定動作を要求したユーザの認証データと、該所定動作によって生成される上記ドキュメントのドキュメントデータと、読み取りを指示した時点のタイムスタンプとをログに記録することを特徴とする請求項９乃至１１のいずれか一項記載の画像形成装置。
【請求項１６】
　上記ドキュメントのネットワーク配信を可能とする上記動作要件を満たしつつ上記所定動作が実行し、実行によって生成されたドキュメントデータをネットワークを介して配信する配信手段を有することを特徴とする請求項１乃至１５のいずれか一項記載の画像形成装置。
【請求項１７】
　ドキュメントの識別情報を読み取る識別情報読取手順と、
　上記識別情報によって指定される動作要件を選択する動作要件選択手順と、
　上記動作要件選択手順によって選択された１つ以上の動作要件に従って所定動作の実行を制御する動作制御手順とを有することを特徴とする画像形成方法。
【請求項１８】
　上記動作要件が実行可能であるか否かを判断する動作要件判断手順と、
　上記動作要件判断手順による判断結果が上記動作要件が実行可能でないことを示す場合、上記所定動作を禁止する動作禁止手順とを有することを特徴とする請求項１７記載の画像形成方法。
【請求項１９】
　ドキュメントの識別情報を読み取る識別情報読取手順と、
　上記識別情報によって指定される動作要件を選択する動作要件選択手順と、
　上記動作要件選択手順によって選択された１つ以上の動作要件に従って所定動作の実行を制御する動作制御手順と、
　上記動作要件が実行可能であるか否かを判断する動作要件判断手順と、
　上記動作要件判断手順による判断結果が上記動作要件が実行可能でないことを示す場合、上記所定動作を禁止する動作禁止手順とをコンピュータに実行させることを特徴とするコンピュータ実行可能可能なプログラム。
【請求項２０】

ドキュメントの識別情報を読み取る識別情報読取手順と、
上記識別情報によって指定される動作要件を選択する動作要件選択手順と、
上記動作要件選択手順によって選択された１つ以上の動作要件に従って所定動作の実行を制御する動作制御手順と、
上記動作要件が実行可能であるか否かを判断する動作要件判断手順と、
上記動作要件判断手順による判断結果が上記動作要件が実行可能でないことを示す場合、上記所定動作を禁止する動作禁止手順とをコンピュータに実行させることを特徴とするプログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

【書類名】明細書
【発明の名称】情報処理装置及び情報処理方法
【技術分野】
【０００１】
本発明は、情報システムのセキュリティを確保するシステムに関し、特に、セキュリティポリシーに基づいたドキュメントの読み取りとネットワーク配信を行う画像形成装置及び画像形成方法に関連する。
【背景技術】
【０００２】
オフィスに代表されるようなドキュメントを扱うフィールドでは、そのドキュメントのセキュリティをコントロールしたいという要望が、常に存在する。例えば秘密の文書を複写する際には管理責任者の許可を得なければならない等，特に情報のコンテナであるドキュメントに対するポリシー，中でも機密保持に関するポリシーの制御が重要視される。一般に、情報システムのセキュリティ確保は機密性、完全性、可用性の確保に大別されるが、完全性や可用性はシステムの管理者が適切に運営、管理すれば実質上問題のないレベルまで確保できることが多い。これに対して、機密性の確保のためには、ユーザ組織に所属するメンバに、ポリシーを共有及び徹底させなければならないためであろうと推測される。
【０００３】
現実に多くの企業では文書管理規定などを設け、セキュリティをコントロールしようとしている。しかし、実際のオフィスシステムにおけるセキュリティの確保については、文書についてのセキュリティではなく、オフィスシステムを構成するさまざまな機器に関して、個別にセキュリティ設定を行う必要がある。
【０００４】
セキュリティポリシーに基づいてアクセス制御を行う方法に関する従来技術としては、種々のものが挙げられる（特許文献１から、特許文献１４）。
【０００５】
例えば、アクセス制御において、条件付のアクセス許可を評価することが記載されている（特許文献１）。
【０００６】
また、例えば、情報セキュリティポリシーに従った企業情報システムのセキュリティ管理、監査の簡単化について記載されている(特許文献２)。
【０００７】
しかし、特に、上述の特許文献１では、データファイルへのアクセス制御システムで、アクセス後のデータの処理、特に読み取りなどには言及されていない。
【０００８】
また、上述の特許文献２では、セキュリティポリシー、システム、制御手段から構成され、それぞれの組み合わせを登録してあるＤＢ（データベース）から制御手段を抽出して、システムをポリシーに合うように制御する手段を有しているがしかし、その状態を監査する手段では、システムに対して登録された制御手段で制御するだけであり、実現の自由度が低い。
【０００９】
また、特許文献７の操作者ＩＤを入力させ、文書からＩＤを取り出し、複写を制御する方法では、複写を拒否する、又は、複写を許可してログを記録するという固定されたルールに基づく制御しか行えない。
【００１０】
特許文献８の画像から機密文書であることを示すマークを取り出してチェックする方法では、得られた情報からどのような動作を行うか否かが決められているため、ルールの柔軟性に欠ける。
【００１１】

特許文献９の印刷情報に含まれる出力制限データに基づいて出力先を制御する方法では、印刷情報にルールを含めなければならない。

【００１２】

特許文献１０の画像を読み取ってパスワードとともに記憶し,出力の際にパスワードが一致したときに許可する方法では、判断する基準がパスワードだけであり、それによって制御される動作も許可、又は、不許可だけである。

【００１３】

特許文献１１のネットワーク上の複数のMFPのうち、一つのMFPがユーザ管理を行ってネットワーク上のMFPすべての操作の許可、不許可を制御する方法では、制御される動作は許可、又は、不許可だけである。

【００１４】

特許文献１２の複数の機器について利用の許可、操作の許可をユーザごとに判断する方法では、許可,不許可だけしか制御できないし、ユーザ情報に基づいた制御しかできない。というように、従来技術の問題点はルールが限定的で柔軟性がなく、またそのルールもあらかじめ決められたものだけであるという欠点がある。すなわち、従来の入出力装置は、「ユーザ」と「ドキュメント」のＩＤに対する、操作の「許可」、「禁止」だけを、「あらかじめ」決められているものばかりである。

【特許文献１】特開２００１－１８４２６４号公報
【特許文献２】特開２００１－２７３３８８号公報
【特許文献３】特開２００１－３３７８６４号公報
【特許文献４】特開平０９－２９３０３６号公報
【特許文献５】特開平０７－１４１２９６号公報
【特許文献６】特許第０２７３５９６６号公報
【特許文献７】特許３２０３１０３号公報
【特許文献８】特開平７－５８９５０号公報
【特許文献９】特開平７－１５２５２０号公報
【特許文献１０】特開平１０－１９１０７２号公報
【特許文献１１】特開２０００－１５８９８号公報
【特許文献１２】特開２０００－３５７０６４号公報
【特許文献１３】特開２００１－１２５７５９号公報
【特許文献１４】特開２００１－３２５２４９号公報。

【発明の開示】

【発明が解決しようとする課題】

【００１５】

このようなセキュリティの実施方法では、ドキュメントの印刷に対するセキュリティを実行する場合には、第１に、セキュリティの施行者が、さまざまな機器のセキュリティに関する知識を必要とする。そして、第２には、すべての機器に対してセキュリティが、一つ一つ実行される必要がある。第３には、システムの全体がどのようなセキュリティ状態になっているのかを容易に把握することが必要であるが、把握しにくい。そして、第４に、個々の機器にセキュリティが実施されていても、実際に文書のセキュリティが守られていることが実感できない。このように、実際のオフィスシステムにおけるセキュリティの確保については、以上のような問題点がある。

【００１６】

本発明は、上述の問題点を解決することを目的とする。

【００１７】

特に本発明の目的は、ドキュメントに関するセキュリティポリシーに基づいて、紙文書の読み取り、ネットワークへの配信を行う画像形成装置、その画像形成装置での処理を実行するプログラム、及び、そのプログラムを記憶した記憶媒体を提供することである。

【課題を解決するための手段】

【００１８】

上記課題を解決するため、本発明は、請求項１に記載されるように、ドキュメントの識別情報を読み取る識別情報読取手段と、上記識別情報によって指定される動作要件を選択する動作要件選択手段と、上記動作要件選択手段によって選択された１つ以上の動作要件に従って所定動作の実行を制御する動作制御手段とを有するように構成される。

【００１９】

このような画像形成装置では、読み取った識別情報で動作要件（動作条件）を選択することができる。すなわち、紙のドキュメントに対して、例えば、組織のセキュリティポリシーに従った動作要件を満たすように印刷、コピー、ＦＡＸ等を制御することができる。

【００２０】

また、本発明は、請求項２に記載されるように、前記動作要件は、上記ドキュメントに対するセキュリティに関する要件であるように構成することができる。

【００２１】

また、本発明は、請求項３に記載されるように、上記所定動作は、電子データで画像を形成するように構成することができる。

【００２２】

また、本発明は、請求項４に記載されるように、上記所定動作は、上記ドキュメントを用紙上に印刷するように構成することができる。

【００２３】

また、本発明は、請求項５に記載されるように、上記識別情報読取手段は、上記ドキュメントに対する所定読み取り動作によって取得したデータを上記識別情報として認識する識別情報認識手段と、上記識別情報とドキュメント属性とを対応付けして管理するドキュメント属性管理手段と、ドキュメント属性管理手段を参照することによって、上記識別情報認識手段よって認識された上記識別情報に対応する上記ドキュメント属性を取得するドキュメント属性取得手段とを有するように構成することができる。

【００２４】

またセキュリティポリシー、本発明は、請求項６に記載されるように、上記所定読み取り動作は、上記ドキュメントが用紙である場合に、該ドキュメントに印字されたバーコード、二次元コード又は磁気コード、又は、該ドキュメントに付与されたＲＦＩＤのいずれかを読み取って上記識別情報として認識するように構成することができる。

【００２５】

また、本発明は、請求項７に記載されるように、上記所定読み取り動作は、上記ドキュメントが用紙である場合に、該ドキュメントを読み取って生成される電子画像データから、バーコード、二次元コード、数字情報、文字情報、ドットパターンのいずれかを上記識別情報として認識するように構成することができる。

【００２６】

また、本発明は、請求項８に記載されるように、上記所定動作を要求するユーザに関するユーザ属性を取得するユーザ属性取得手段を更に有するように構成することができる。

【００２７】

また、本発明は、請求項９に記載されるように、上記ユーザ属性取得手段は、上記ユーザから該ユーザを識別するユーザ識別情報を取得するユーザ識別情報取得手段と、該ユーザ識別情報と上記ユーザ属性とを対応付けして管理するユーザ属性管理手段と、上記ユーザ識別情報に基づいて上記ユーザを認証するユーザ認証手段と、上記ユーザ認証手段による認証結果に基づいて、上記ユーザ属性管理手段を参照することによって、上記ユーザ識別情報取得手段によって取得された上記ユーザ識別情報に対応する上記ユーザ属性を取得するユーザ属性取得手段とを有するように構成することができる。

【００２８】

また、本発明は、請求項１０に記載されるように、上記ユーザ属性取得手段は、上記ユーザから該ユーザを識別するユーザ識別情報を取得するユーザ識別情報取得手段と、上記ユーザを認証し、上記ユーザ属性を提供する外部サーバに対して該ユーザ属性を要求するユーザ属性要求手段とを有するように構成することができる。

【００２９】
また、本発明は、請求項１１に記載されるように、上記動作要件が実行可能であるか否かを判断する動作要件判断手段と、上記動作要件判断手段による判断結果が上記動作要件が実行可能でないことを示す場合、上記所定動作を禁止する動作禁止手段とを有するように構成することができる。
【００３０】
また、本発明は、請求項１２に記載されるように、上記動作要件は、上記ドキュメント対する上記所定動作の実行の際に、電子透かしを埋め込むことを指示するように構成することができる。
【００３１】
また、本発明は、請求項１３に記載されるように、上記動作要件は、上記ドキュメント対する上記所定動作の実行の際に、表示可能なラベルを埋め込むことを指示するように構成することができる。
【００３２】
また、本発明は、請求項１４に記載されるように、上記表示可能なラベルは、少なくとも上記所定動作を要求したユーザの認証データと、上記所定動作を要求した時点のタイムスタンプを含むように構成することができる。
【００３３】
また、本発明は、請求項１５に記載されるように、上記動作要件は、上記ドキュメント対する上記所定動作の実行の際に、少なくとも上記所定動作を要求したユーザの認証データと、該所定動作によって生成される上記ドキュメントのドキュメントデータと、読み取りを指示した時点のタイムスタンプとをログに記録するように構成することができる。
【００３４】
また、本発明は、請求項１６に記載されるように、上記ドキュメントのネットワーク配信を可能とする上記動作要件を満たしつつ上記所定動作が実行し、実行によって生成されたドキュメントデータをネットワークを介して配信する配信手段を有するように構成することができる。
【００３５】
上記課題を解決するための手段として、本発明は、上記画像形成装置での処理をコンピュータに行なわせるための画像形成方法及びプログラム、及び、そのプログラムを記憶したコンピュータ読み取り可能な記憶媒体とすることもできる。
【発明の効果】
【００３６】
本願発明によれば、情報システムのセキュリティを確保するシステムに関し、特に、セキュリティポリシーに基づいたドキュメントの読み取りとネットワーク配信を行う画像形成装置及び画像形成方法を提供することができる。
【発明を実施するための最良の形態】
【００３７】
以下、本発明の実施の形態を図面に基づいて説明する。
【００３８】
本発明の実施例を、以下に詳細に説明する。
【００３９】
本実施例では、異なるタイプのシステムでドキュメントに対するセキュリティポリシーを共有するために、以下のような仕組みを使用して、セキュリティポリシーを記述する。ここでは、記述したセキュリティポリシーのことをドキュメントセキュリティポリシー（ＤＳＰ）と呼ぶ。
【００４０】
図１は、セキュリティポリシーの例を示す。ユーザの属する組織は、例えば、機密文書、丸秘文書、社外秘文書のような、文書の機密レベルごとに、ドキュメントに対して、例えば、図１のようなセキュリティポリシーを掲げることが想定される。

【００４１】
このようなポリシーをＤＳＰとして記述できるようにするために，以下のような方法を使用する。
【００４２】
まず最初に、ドキュメントを機密レベル（極秘、丸秘、社外秘など）と、カテゴリー（人事文書、技術文書など）に応じて分類する。この、機密レベルとカテゴリーの組みを、ドキュメントのセキュリティラベルと呼ぶ。このセキュリティラベルは、実際には、個々のドキュメントに属性情報として付与される。
【００４３】
上記のような、分類の仕方の一例を図２に示す。図２は、ドキュメントラベル用語ファイルの例を示す。図２に示されるようなドキュメントラベル用語ファイル３００は、個々のドキュメントに属性情報として付与されるラベルのリストを管理するファイルであり、例えば、ＸＭＬによって記述される。
【００４４】
ＤＳＰには、ドキュメントの機密レベル及びカテゴリーに応じて、ドキュメントに対して許可される操作（オペレーション）を規定し、そして、その操作を許可する際に実行されるべき要件（管理責任者の許可を得る、ラベルを印刷する、など）を指定できるようにする必要がある。そのような、ドキュメントの機密レベル及びカテゴリーを記述するのが、図２のドキュメントラベル用語ファイル３００である。
【００４５】
図２において、<enumeration>から</enumeration>で示される記述３１１及び記述３２１によって、２種類のカテゴリーが示される。
【００４６】
記述３１１において、<enum_id>doc_category</enum_id>を示す記述３１２は、カテゴリーの識別情報が「doc_category」であることを示す。<enum_name>Document Category</enum_name>を示す記述３１３は、カテゴリーの名称が「Document Category」であることを示す。<description>文書カテゴリーの種類</description>を示す記述３１４は、このカテゴリーが何を分類するか示す説明「文書カテゴリーの種類」を示す。
【００４７】
<item>から</item>を示す記述３１５、記述３１６及び記述３１７によって、３つのカテゴリーの項目が示される。記述３１５は、<name>internal_doc</name>を示す記述によって、項目名が「internal_doc」であることを示し、<description>社内一般文書</description>を示す記述によって、その項目の説明「社内一般文書」を示す。
【００４８】
記述３１６は、<name>human_resource_doc</name>を示す記述によって、項目名が「human_resource_doc」であることを示し、<description>人事関連文書</description>を示す記述によって、その項目の説明「人事関連文書」を示す。
【００４９】
記述３１７は、<name>technical_doc</name>を示す記述によって、項目名が「technical_doc」であることを示し、<description>技術関連文書</description>を示す記述によって、その項目の説明「技術関連文書」を示す。
【００５０】
同様に、記述３２１において、<enum_id>doc_security_level</enum_id>を示す記述３２２は、カテゴリーの識別情報が「doc_security_level」であることを示す。<enum_name>Document Security Level</enum_name>を示す記述３２３は、カテゴリーの名称が「Document Security Level」であることを示す。<description>文書のセキュリティレベルの種類</description>を示す記述３２４は、このカテゴリーが何を分類するか示す説明「文書のセキュリティレベルの種類」を示す。
【００５１】
<item>から</item>を示す記述３２５、記述３２６及び記述３２７によって、３つのカ

テゴリーの項目が示される。記述３２５は、<name>basic</name>を示す記述によって、項目名が「basic」であることを示し、<description>社外秘</description>を示す記述によって、その項目の説明「社外秘」を示す。

【００５２】

記述３２６は、<name>medium</name>を示す記述によって、項目名が「medium」であることを示し、<description>秘</description>を示す記述によって、その項目の説明「秘」を示す。

【００５３】

記述３２７は、<name>high</name>を示す記述によって、項目名が「high」であることを示し、<description>極秘</description>を示す記述によって、その項目の説明「極秘」を示す。

【００５４】

このように、ドキュメントラベル用語ファイル３００によって、社内一般文書、人事関連文書及び技術関連文書のような、文書カテゴリーの種類が規定される。また、社外秘、秘、極秘のような、文書のセキュリティレベルの種類が規定される。

【００５５】

図３から図１３は、ポリシー用語ファイルの例を示す図を示す。図３から図１３により、１つのポリシー用語ファイル４００を構成する。

【００５６】

図３から図１３に示されるようなポリシー用語ファイル４００は、システムタイプの分類を記述し、そのシステムタイプごとに、オペレーションを列挙する。そして、そのオペレーションごとに、オペレーションの実行の際にサポート可能な要件を列挙しておく。ポリシー用語ファイル４００は、例えば、ＸＭＬによって記述される。

【００５７】

図３において、列挙して記述する方法は、図２に示すドキュメントラベルファイル３００での記述方法と同様に<enumeration>から</enumeration>までの記述を繰り返すことによって示される。<enumeration>から</enumeration>までの詳細な記述は、図２に示すドキュメントラベルファイル３００での記述方法と同様であるので、ここでは、簡単な説明のみとする。

【００５８】

例えば、図３においては、記述４１１によってシステムタイプが列挙される。記述４１１によると、「システムタイプの種類」として、「複写機」、「プリンタ」、「ファクシミリ」、「スキャナ」、「文書リポジトリ」、及び、「電子会議システム」が記述される。

【００５９】

そして、例えば、図４に示されたように、記述４２１から記述４７１によってシステムタイプごとの各オペレーションが列挙される。

【００６０】

記述４２１において、「複写機に関わるオペレーション」として、「紙から紙への複写」が記述される。記述４３１において、「プリンタに係わるオペレーション」として、「電子文書を紙へ印刷」が記載される。記述４４１において、「ファックスに関わるオペレーション」として、「ファックス送信」及び「ファックス受信」が記載される。記述４５１において、「スキャナに関わるオペレーション」として、「紙文書をスキャンして電子文書にする」が記載される。

【００６１】

記述４６１において、「文書リポジトリに関わるオペレーション」として、「保存する」、「改訂・編集する」、「削除・破棄する」、「参照する」、「ネットワークで配布する（送信する）」、「ディスクで配布する（送付する）」、及び、「アーカイブ・バックアップする」が記述される。記述４７１において、「電子会議システムに関わるオペレーション」として、「会議で利用する」が記述される。

【００６２】
更に、例えば、図６から図１３示すように、記述４８１から記述６０１によってオペレーション毎に適用できる要件が列挙される。
【００６３】
記述４８１において、「複写に関わる要件」として、「明示的な許可」、「監査証跡の記録」、及び、「監査証跡のイメージ付き記録」が記載される。
【００６４】
記述４９１において、「印刷に関わる要件」として、「明示的な許可（利用制限）」、「監査証跡の記録」、「監査証跡のイメージ付き記録」、「プリントした本人による紙出力」、「信頼チャネルの利用（印刷データの暗号化）」、及び、「プリントアウトに追跡情報埋め込み（透かし、ラベル、バーコード）」が記載される。
【００６５】
記述５０１において、「ファックス送信に関わる要件」として、「明示的な許可（利用制限）」、「監査証跡の記録」、「監査証跡のイメージ付き記録」、「宛先制限」、「親展モードでの送信」、「信頼チャネルの利用」、「送信ファックスに追跡情報埋め込み（透かし、ラベル、バーコード）」、及び、「否認防止（受取証の取得）」が記載される。
【００６６】
記述５１１において、「ファックス受信に関わる要件」として、「監査証跡の記録」、「監査証跡のイメージ付き記録」、「親展ファックスの宛先本人による取り出し」、「信頼タイムスタンプ」、及び、「受信ファックスに追跡情報埋め込み（透かし、ラベル、バーコード）」が記載される。
【００６７】
記述５２１において、「スキャンに関わる要件（保存した後については保存要件を適用する）」として、「明示的な許可（利用制限）」、「監査証跡の記録」、「監査証跡のイメージ付き記録」、及び、「スキャン画像に追跡情報埋め込み（透かし、ラベル、バーコード）」が記載される。
【００６８】
記述５３１において、「保存に関わる要件」として、「明示的な許可（利用制限）」、「監査証跡の記録」、「保存データの暗号化」、及び、「保存データの改ざん保護」が記載される。
【００６９】
記述５４１において、「改訂に関わる要件」として、「明示的な許可（利用制限）」、「監査証跡の記録」、及び、「バージョン管理」が記載される。
【００７０】
記述５５１において、「削除・破棄に関わる要件」として、「明示的な許可（利用制限）」、「監査証跡の記録」、「監査証跡のイメージ付き記録」、及び、「完全消去」が記載される。
【００７１】
記述５６１において、「参照に関わる要件」として、「明示的な許可（利用制限）」、「監査証跡の記録」、「編集禁止のデータのみ参照許可」、「印刷禁止のデータのみ参照許可」、「参照場所限定のデータのみ参照許可」、及び、「ユーザ限定のデータのみ参照許可」が記載される。
【００７２】
記述５７１において、「ネットワーク配信（送信）に関わる要件」として、「明示的な許可（利用制限）」、「監査証跡の記録」、「監査証跡のイメージ付き記録」、「信頼チャネルの利用（送信データの暗号化）」、「宛先制限（社内のみ配信可能など）」、「編集禁止のデータのみ配信許可」、「印刷禁止のみ配信許可」、「参照場所限定のデータのみ配信許可」、及び、「ユーザ限定のデータのみ配信許可」が記載される。
【００７３】
記述５８１において、「ディスク配布（送付）に関わる要件」として、「明示的な許可

（利用制限）」、「監査証跡の記録」、「監査証跡のイメージ付き記録」、「送付データの暗号化」、「送付データの改ざん保護」、「編集禁止のデータのみ送付許可」、「印刷禁止のみ送付許可」、「参照場所限定のデータのみ送付許可」、及び、「ユーザ限定のデータのみ送付許可」が記載される。

【００７４】

記述５９１において、「アーカイブ・バックアップに関わる要件」として、「明示的な許可（利用制限）」、「監査証跡の記録」、「アーカイブデータの暗号化」、及び、「アーカイブデータの改ざん保護」が記載される。

【００７５】

記述６０１において、「会議での利用に関わる要件」として、「明示的な許可（利用制限）」、「監査証跡の記録」、及び、「監査証跡のイメージ付き記録」が記載される。

【００７６】

図２のドキュメントラベル用語ファイルと図３から図１３のポリシー用語ファイルとに基づくＤＳＰについて図１４から図２２で説明する。図１４から図２２は、ポリシーファイルの例を示す図である。上述の図２に示すドキュメントラベル用語ファイル３００と、図３から図１３のポリシー用語ファイル４００とに基づいて、ユーザの組織内でのセキュリティに対するポリシーが、例えば図１４から図２２に示すＤＳＰ２０００のようにＸＭＬで記述され、１つのポリシーファイルを構成する。

【００７７】

図１４から図２２に示されるようなＤＳＰ２０００は、<policy>で示される記述２００１から</policy>で示される記述２００２にてポリシーが示される。

【００７８】

図１４の<acc_rule>を示す記述２０１１から図１６の</acc_rule>を示す記述２０１２において、<doc_category>ANY</doc_category>及び<doc_security_level>basic</doc_security_level>を示す記述２０１３によって、ドキュメントカテゴリ「ANY（非限定）」かつドキュメントセキュリティレベル「basic（基本レベル）」であるドキュメント属性を有するドキュメントに対して、<user_category>ANY</user_category>及び<user_security_level>ANY</user_security_level>を示す記述２０１７によって、ユーザカテゴリ「ANY（非限定）」かつユーザセキュリティレベル「ANY（非限定）」であるユーザ属性を有するユーザが行うオペレーション毎のポリシーが記述される。<operation>から</operation>までの記述毎に、オペレーションの許可（<allowed/>）又は不許可（<denied/>）が規定される。更に、オペレーションが許可される場合は、許可するための要件（<requirement>）が規定される。

【００７９】

図１６の<acc_rule>を示す記述２０２１から図１９の</acc_rule>を示す記述２０２２において、<doc_category>ANY</doc_category>及び<doc_security_level>medium</doc_security_level>を示す記述２０２３によって、ドキュメントカテゴリ「ANY（非限定）」かつドキュメントセキュリティレベル「medium（中レベル）」であるドキュメント属性を有するドキュメントに対して、<user_category>DOC-CATEGORY</user_category>及び<user_security_level>ANY</user_security_level>を示す記述２０２７によって、ユーザカテゴリ「DOC-CATEGORY（文書カテゴリーの種類）」（図２の記述３１２、３１３及び３１４参照）かつユーザセキュリティレベル「ANY（非限定）」であるユーザ属性を有するユーザが行うオペレーション毎のポリシーが記述される。<operation>から</operation>までの記述毎に、オペレーションの許可（<allowed/>）又は不許可（<denied/>）が規定される。更に、オペレーションが許可される場合は、許可するための要件（<requirement>）が規定される。

【００８０】

また、同様のドキュメント属性を有するドキュメントに対して、図１８の<user_category>ANY</user_category>及び<user_security_level>ANY</user_security_level>を示す記述２０２８によって、ユーザカテゴリ「ANY（非限定）」かつユーザセキュリティレベル

「ANY（非限定）」であるユーザ属性を有するユーザが行うオペレーション毎のポリシーが記述される。<operation>から</operation>までの記述毎に、オペレーションの許可（<allowed/>）又は不許可（<denied/>）が規定される。更に、オペレーションが許可される場合は、許可するための要件（<requirement>）が規定される。

【００８１】

図１９の<acc_rule>を示す記述２０３１から図１９の</acc_rule>を示す記述２０３２において、<doc_category>ANY</doc_category>及び<doc_security_level>high</doc_security_level>を示す記述２０２３によって、ドキュメントカテゴリ「ANY（非限定）」かつドキュメントセキュリティレベル「high（高レベル）」であるドキュメント属性を有するドキュメントに対して、<user_category>DOC-CATEGORY</user_category>及び<user_security_level>ANY</user_security_level>を示す記述２０３７によって、ユーザカテゴリ「DOC-CATEGORY（文書カテゴリーの種類）」（図２の記述３１２、３１３及び３１４参照）かつユーザセキュリティレベル「ANY（非限定）」であるユーザ属性を有するユーザが行うオペレーション毎のポリシーが記述される。<operation>から</operation>までの記述毎に、オペレーションの許可（<allowed/>）又は不許可（<denied/>）が規定される。更に、オペレーションが許可される場合は、許可するための要件（<requirement>）が規定される。

【００８２】

次に、図１４から図２２のＤＳＰ２０００の構造を、図２３から図２５を参照して、以下に、詳しく説明する。

【００８３】

図２３は、ＤＳＰの識別情報の例を示す図である。ＤＳＰ２０００の識別情報２１０において、＜about_this_policy＞と＜/about_this_policy＞とで囲まれた範囲の記述２１１～２１３には、ＤＳＰ２０００を識別するための識別情報が記述される。

【００８４】

<serial_number>RDSP2023</serial_number>を示す記述２１１には、ＤＳＰ２０００を他のＤＳＰと区別するためのシリアル番号が記述される。

【００８５】

<terminology_applied>RDST9487</terminology_applied>で示される記述２１２には、ＤＳＰ２０００に対応するポリシー用語ファイル４００のシリアル番号が記述される。尚、この定義ファイルは更新される可能性があるため、このＤＳＰ２０００がどのポリシー用語ファイルに基づいて記述されているのかを明確にするために記録しておく。記述２１３には、<title> DOCUMENT-SECURITY-POLICY</title>を示す記述によってＤＳＰ２０００のタイトル、<version>1.20</version>を示す記述によってバージョン番号、<creation_date>2002/02/18 22:30:24</creation_date>を示す記述によって作成日時、<creator>Taro Tokyo</creator>を示す記述によって作成者、<description>sample document security policy.</description>を示す記述によって説明などの一般的な書誌情報が記述される。

【００８６】

そして、ＤＳＰ２０００の識別情報は、</about_this_policy>により終了する。

【００８７】

次に、上述のＤＳＰ２００の識別情報に続いて、ポリシーの内容を<policy>と</policy>で囲まれた範囲に記述する。図２４は、ＤＳＰの構造を説明するための記述例を示す図である。

【００８８】

図２４に示されるポリシーの内容２２０は、以下に説明するように、階層構造を用いて記録する。

【００８９】

ポリシー<policy>は、複数のアクセス制御ルール<acc_rule>（記述２２１）で構成される。一つのアクセス制御ルール<acc_rule>（記述２２１）は、対象とするドキュメントのカテゴリー<doc_category>とレベル<doc_security_level>を一意に指定し（記述２２２）

，さらにアクセス制御リスト<acl>（記述２２３）を一つ含むように構成される。

【００９０】

アクセス制御リスト<acl>（記述２２３）は、複数のアクセス制御エレメント<ace>（記述２２４）で構成される。

【００９１】

各アクセス制御エレメント<ace>（記述２２４）は、対象とするユーザのカテゴリー<user_category>（記述２２５）とレベル<user_security_level>（記述２２６）を一意に指定し，さらに複数のオペレーション<operation>（記述２２７）で構成される。

【００９２】

各<operation>（記述２２７）は、一つのオペレーション名<name>（記述２２８）と、一つの禁止<denied/>（記述２２９）、または一つの許可<allowed/>（記述２３２）、または複数の<requirement>（記述２３０及び記述２３１）で構成される。

【００９３】

記述２２２において、ドキュメントのカテゴリー<doc_category>やユーザのカテゴリー<user_category_level>に記述している”ANY”は、どのカテゴリー、及び、レベルにも適用されることを示している。また、記述２２５によって示されるユーザのカテゴリー<user_category>の”DOC-CATEGORY”は、ユーザのカテゴリーがドキュメントのカテゴリーと同じときに適用されることを示している。

【００９４】

この実施例では、禁止するオペレーションには<denied/>（記述２２９）を指定するようにしているが、ＤＳＰ２０００に記載されていなければアクセスは許可されていないことを表している、というように構成してもよい。

【００９５】

このように、ＤＳＰを記述することにより、ドキュメントのタイプ（カテゴリー、レベル）に応じて，どのようなユーザタイプ（カテゴリー、レベル）が、ドキュメントに対してどのようなオペレーションが可能なのかを記述できる。そして更に、そのドキュメントについて、ユーザが、オペレーションが可能な場合には、どのような要件を満たさなければならないのかを明確に記述することができる。

【００９６】

そして、ＤＳＰを、上記のようにプラットフォームに依存しないXMLで記述することにより、異なるタイプのシステム間で、このＤＳＰを共通に利用することができる。特に、セキュリティポリシーを適用したい対象は、電子的なドキュメントに限らず、紙のドキュメントに対しても適用できなければならないため、図３から図１３のドキュメントラベルファイルや図１４から図２２のＤＳＰ２０００に記述しているように、紙ドキュメントに関するオペレーション（hardcopy，scanなど）も規定できる。

【００９７】

本実施例の、図２４に示す要件の中に、以下の<requirement>explicit_authorization</requirement>を示す記述２３１が存在する。これは、「ドキュメントの管理責任者により明示的な許可が得られた場合には、そのオペレーションを許可する」という要件である。すべて、このＤＳＰに従ってオペレーションがコントロールされるようになると、自由度が無くなる恐れが生じる。しかし、この明示的な許可という要件を指定できるようにすることにより、柔軟なオペレーションコントロールが可能となる。

【００９８】

また、本実施例の特徴として、その「明示的な許可」という要件を指定可能にすることによって、明示的な許可が得られれば実行してもよいオペレーションと，明示的な許可が得られたとしても禁止しなければならないオペレーションとを区別することができるということである。

【００９９】

従って、ＤＳＰに記載しないか又は、<denied/>で指定されたオペレーションは明示的な許可が得られたとしても禁止しなければならないオペレーションである。これにより、

ポリシーを記述している側の意図を、的確に規定できるようになり、誤って許可を与えてしまってオペレーションが実行されてしまうというような事態をあらかじめ防ぐように規定することができる。

【０１００】

次に本発明のＤＳＰの別の記述形を図２６で説明する。図２５は、ＤＳＰの他の記述例を示す図である。図２６に示すポリシーの内容２４０は、無条件で許可するオペレーションや、禁止するオペレーションが多くなった場合には、オペレーションごとに<operation><allowed/></operation>というような入れ子構造を記述するのは効率が悪いので、無条件で許可するオペレーションを列挙する、<allowed_operations>を示す記述２４３と、許可しないオペレーションを列挙する、<denied_operations>を示す記述２４１を使用するようにしても良い。

【０１０１】

また、<requirement>explicit_authorization</requirement>を示す記述２４２は、図２４での説明と同様である。

【０１０２】

図２６は、上述のＤＳＰを蓄積し且つ配布する種々の媒体を示す。

【０１０３】

以上で説明したように、図２６に示されたＤＳＰ２０００は、XML（Ｅｘｔｅｎｓｉｂｌｅ　Ｍａｒｋｕｐ　Ｌａｎｇｕａｇｅ）で記述されている。そして、電子的なファイルとして記録しておくことができる。また、その電子的なファイルを格納した、例えば、ハードディスク５１、光磁気ディスク５２、フレキシブルディスク５３、又は、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、ＣＤ－ＲＷ、ＤＶＤ、ＤＶＤ－Ｒ、ＤＶＤ－ＲＡＭ、ＤＶＤ－ＲＷ、ＤＶＤ＋ＲＷ、ＤＶＤ＋Ｒのような光ディスク５４のような記憶媒体を作成することができる。また、その電子的なＤＳＰ２０００をコンピュータ５５を使用して、ネットワーク５６を介してで伝送することができる。

【０１０４】

このＤＳＰ２０００は、特定のシステム向けのセキュリティポリシーの記述ではなく、異なる複数のシステムで共通に利用できるセキュリティポリシーの記述である。従って、このセキュリティポリシー記述を記憶した記憶媒体を作成し、そして配布したり又は、ネットワーク経由して伝送したりすることにより、複数のシステムで共通に利用しやすくなる。

【０１０５】

図２７は、本発明の一実施例に係る画像形成装置のハードウェア構成を示すブロック図である。図２７において、画像形成装置１０００は、コンピュータによって制御される装置であって、ＣＰＵ（中央処理装置）１１と、ＲＯＭ（Read-Only Memory）１２と、ＲＡＭ（Random Access Memory）１３と、不揮発性ＲＡＭ（non-volatile Random Access Memory）１４と、リアルタイムクロック１５、イーサネット（登録商標）Ｉ／Ｆ（Ethernet（登録商標） Interface）２１と、ＵＳＢ（Universal Serial Bus）２２と、ＩＥＥＥ（Institute of Electrical and Electronics Engineers）1284 ２３と、ハードディスクＩ／Ｆ２４と、エンジンＩ／Ｆ２５と、ＲＳ－２３２Ｃ　Ｉ／Ｆ２６と、ドライバ２７とで構成され、システムバスＢに接続される。

【０１０６】

ＣＰＵ１１は、ＲＯＭ１２に格納されたプログラムに従って画像形成装置１０００を制御する。ＲＡＭ１３には、例えば、各インターフェース２１から２６に接続される資源に領域が割り当てられる。不揮発性ＲＡＭ１４には、画像形成装置１０００を制御するためにＣＰＵ１１による処理で必要な情報が格納される。リアルタイムクロック１５は、現時刻を計ると共に、処理を同期させる場合にＣＰＵ１１によって使用される。

【０１０７】

イーサネット（登録商標）Ｉ／Ｆ２１には、１０ＢＡＳＥ－Ｔ又は１００ＢＡＳＥ－ＴＸ等のイーサネット（登録商標）用インターフェースケーブルが接続される。ＵＳＢ２２

には、ＵＳＢ用インターフェースケーブルが接続される。ＩＥＥＥ1284 ２３には、ＩＥＥＥ1284用インターフェースケーブルが接続される。

【０１０８】

ハードディスクＩ／Ｆ２４には、ハードディスク３４が接続され、ネットワークを介して送信された印刷すべき文書の文書データ、又は、印刷処理後の画像データがハードディスクＩ／Ｆ２４を介してハードディスク３４に格納される。エンジンＩ／Ｆ２５には、文書データに基づいて所定媒体に印刷を行うプロッタ３５－１及び画像データを取り込むスキャナ３５－２等が接続される。ＲＳ－２３２Ｃ　Ｉ／Ｆ２６には、オペレーションパネル３６が接続され、ユーザへの情報の表示及びユーザから入力情報又は設定情報の取得が行われる。

【０１０９】

画像形成装置１０００によって行われる処理を実現するプログラムは、例えば、ＣＤ－ＲＯＭ等の記憶媒体３７によって画像形成装置１０００に提供される。即ち、プログラムが保存された記憶媒体３７がドライバ２７にセットされると、ドライバ２７が記憶媒体３７からプログラムを読み出し、その読み出されたプログラムがシステムバスＢを介してハードディスク３４にインストールされる。そして、プログラムが起動されると、ハードディスク３４にインストールされたプログラムに従ってＣＰＵ１１がその処理を開始する。尚、プログラムを格納する記憶媒体３７としてＣＤ－ＲＯＭに限定するものではなく、コンピュータが読み取り可能な記憶媒体であればよい。プログラムをネットワークを介してダウンロードし、ハードディスク３４にインストールするようにしても良い。

【０１１０】

セキュリティポリシーに従って動作する画像形成装置について図２８、図２９及び図３０を参照して以下に詳細に説明する。

【０１１１】

図２８は、セキュリティポリシーに従って動作する読み取り装置としての画像形成装置の機能構成を示す図である。

【０１１２】

図２８に示す読み取り装置としての画像形成装置１０００は、主に、読み取り部７１と、読み取り条件取得部７２と、データ送信先取得部７３と、データ処理部７４と、データ送信部７５と、ポリシー実行部１００１と、読み取り画像データ６１と、蓄積データ６２とを有する。

【０１１３】

また、ポリシー実行部１００１は、ドキュメント属性取得部１０１１と、動作要件選択部１０１２と、動作制御部１０１３と、ユーザ属性取得部１０２１とを有する。ドキュメント属性取得部１０１１は紙原稿６０から又は読み取り画像データ６１からドキュメント属性を取得して、動作要件選択部１０２１へ通知する。

【０１１４】

一方、ユーザ属性取得部１０２１は、ユーザによって入力されたユーザ情報を取得すると、動作要件選択部１０１２に通知する。動作要件選択部１０１２は、ＤＳＰ２０００に従って許可される場合の要件を選択し、その結果を動作制御部１０１３に通知する。動作制御部１０１３は、読み取った紙原稿６０の画像データに対するデータ処理を指示する。

【０１１５】

ポリシー実行部１００１において、点線で示される部分について省略しても良い。

【０１１６】

読み取り部７１は、読み取り条件取得部７２から通知されるユーザによって入力された読み取り条件に従って、紙原稿６０を読み取る（スキャン）する処理部であり、読み取った画像データは、読み取り画像データ６１に格納される。また、画像データ６１から取得したドキュメント属性をドキュメント属性取得部１０１１に通知する。

【０１１７】

読み取り条件取得部７２は、ユーザによって入力された読み取り条件を取得し、読み取

り部７１とデータ処理部７４とへ通知する。

【０１１８】

データ送信先取得部７３は、ユーザによって入力されたデータ送信先を取得し、データ送信部７５に通知すする処理部である。

【０１１９】

データ処理部７４は、動作制御部１０１３から提供される要件を満たすように読み取り条件取得部７２から通知されるユーザによって入力された読み取り条件に従って、データ処理を読み取った画像データに行い、データ処理された画像データを蓄積データ６２に蓄積する。

【０１２０】

データ送信部７５は、動作制御部１０１３から通知される要件を満たすように、蓄積データ６２から取り出した処理対象となる画像データをデータ送信先取得部７３から通知された送信先へ送信する。

【０１２１】

画像データを外部に送信する必要がない場合、データ送信部２８を省略しても良い。また、画像データを記憶媒体３７に記憶するようにしても良い。

【０１２２】

図２８において、読み取り装置としての画像形成装置１０００は、専用のハードウェアにより構成するように記載されているが、汎用のコンピュータとそのコンピュータ上で実行されるプログラムにより構成されても良い。

【０１２３】

また、以下に説明する本発明の実施例をコンピュータ上で実行するプログラムは、コンピュータにより読み出し可能な記憶媒体に記録され、その実行前に、コンピュータにより読みこまれる。また、このようなプログラムは、コンピュータネットワークを介して配信されることも可能である。

【０１２４】

図２９は、簡略化したＤＳＰの例を示す図である。説明の便宜のため、ＤＳＰ２０００を簡略化したＤＳＰで説明する。図２９に示されるＤＳＰ２１００において、つぎのようにルール１からルール３を示す。

【０１２５】

ルール１は、図２９の第４行目の<acc_rule>から、第１０行目の<user_security_level>ANY</user_security_level>までの部分及び、第１１行目<operation>から、第１４行目</operation>までの部分により記述される。

【０１２６】

第５行目の <doc_category>ANY</doc_category>は、文書カテゴリーにかかわりなくルール１が適用されることを示す。

【０１２７】

第６行目の<doc_security_level>basic</doc_security_level>は、文書のセキュリティレベルがbasicのときを示す。

【０１２８】

第９行目の<user_category>ANY</user_category>は、ユーザのカテゴリーにかかわりないことを示す。

【０１２９】

第１０行目の<user_security_level>ANY</user_security_level>は、ユーザのセキュリティレベルにかかわりないことを示す。

【０１３０】

更に第１２行目と第１３行目の<name>scan</name>及び<allowed/>は、読み取りは要件なく許可されることを示す。

【０１３１】

従って、ルール１では、第５行目、第６行目、第９行目、第１０行目、第１２行目及び

第１３行目により、文書カテゴリーにかかわりなく、文書のセキュリティレベルが”basic”の場合には、ユーザのカテゴリーにかかわりなく、且つ、ユーザのセキュリティレベルにかかわりなく、読み取りは要件なく許可される。

【０１３２】

次に、ルール２は、図２９の第４行目の<acc_rule>から、第１０行目の<user_security_level>ANY</user_security_level>までの部分及び、第１５行目<operation>から、第２０行目</operation>までの部分により記述される。

【０１３３】

第５行目の <doc_category>ANY</doc_category>は、文書カテゴリーにかかわりなくルール２が適用されることを示している。

【０１３４】

第６行目の<doc_security_level>basic</doc_security_level>は、文書のセキュリティレベルがbasicのときを示す。

【０１３５】

第９行目の<user_category>ANY</user_category>は、ユーザのカテゴリーにかかわりないことを示す。

【０１３６】

第１０行目の<user_security_level>ANY</user_security_level>は、ユーザのセキュリティレベルにかかわりないことを示す。

【０１３７】

更に、第１６行目から第１９行目の

<name>net_delivery</name>
<requirement>audit</requirement>
<requirement>print_restriction</requirement>
<requirement>trusted_channel</requirement>

は、ネットワーク配信は、「ログを記録すること」と、「プリント制限をかけること」、「信頼できるチャネルを使用すること」の要件を満たすときに許可されることを示す。

【０１３８】

従って、ルール２では、第５行目、第６行目、第９行目、第１０行目、第１６行目から第１９行目により、文書カテゴリーにかかわりなく、文書のセキュリティレベルが”basic”の場合には、ユーザのカテゴリーにかかわりなく、且つ、ユーザのセキュリティレベルにかかわりなく、ネットワーク配信は、ログを記録することと、プリント制限をかけること、信頼できるチャネルを使用することの要件を満たすときに許可されることを示している。

【０１３９】

そして、ルール３は、図２９の第２４行目の<acc_rule>から、第３０行目の<user_security_level>ANY</user_security_level>までの部分及び、第３１行目<operation>から、第３５行目</operation>までの部分により記述される。

【０１４０】

第２５行目の<doc_category>ANY</doc_category>は、文書カテゴリーにかかわりないことを示す。

【０１４１】

第２６行目の<doc_security_level>high</doc_security_level>は、
文書のセキュリティレベルがhighの場合を示す。

【０１４２】

第２９行目の<user_category>DOC-CATEGORY</user_category>は、ユーザのカテゴリーが文書のカテゴリーと同じであることを示す。

【０１４３】

第３０行目の<user_security_level>ANY</user_security_level>は、ユーザのセキュリティレベルにかかわりないことを示す。

【０１４４】
第３２行目から第３４行目の、
<name>scan</name>
<requirement>audit</requirement>
<requirement>embed_trace_info</requirement>
は、読み取りは、「ログを記録すること」及び、「追跡可能な情報を埋め込むこと」の要件を満たすときに許可される。
【０１４５】
従って、ルール３では、第２５行目、第２６行目、第２９行目、第３０行目、第３１行目から第３４行目により、文書カテゴリーにかかわりなく、文書のセキュリティレベルが”high”の場合には、ユーザのカテゴリーが文書のカテゴリーと同じであり、且つ、ユーザのセキュリティレベルにかかわりなく、読み取りは、ログを記録することと、追跡可能な情報を埋め込むことの要件を満たすときに許可されることを示している。
【０１４６】
ここで、「追跡可能な情報を埋め込むこと」には、例えば、電子すかしの埋め込み、表示可能なラベルの埋め込み、文書属性情報の追加などを含んでも良い。また、表示可能なラベルは、読み取りを指示したユーザの認証データと読み取りを指示した時点のタイムスタンプを含んでもよい。さらに、「ログを記録すること」には、読み取りを指示したユーザの認証データと、読み取り対象の文書データと、読み取りを指示した時点のタイムスタンプをログに記録するようにしてもよい。また、「ログを記録すること」には、ネットワーク配信を指示したユーザの認証データとネットワーク配信先の情報と、読み取り対象の文書データと、読み取りを指示した時点のタイムスタンプをログに記録するようにしてもよい。
【０１４７】
図２８を参照しつつ、詳細な動作について説明する。
【０１４８】
上述の図２９に示すＤＳＰ２１００に基づいて、例えば、セキュリティレベルが”basic”の文書を読み取りしようとしている場合には、抽出すべき要件はない。
【０１４９】
また、上述の図２９に示すセキュリティポリシーに基づいて、例えば、セキュリティレベルが”high”の文書を読み取りしようとしている場合には、前述のように、「ログを記録すること」及び「追跡可能な情報を埋め込むこと」が、読み取りの要件となる。「ログを記録すること」及び「追跡可能な情報を埋め込むこと」の内容に関しては、上述と同様である。
【０１５０】
次に、セキュリティレベルが”basic”のときの場合のように、抽出すべき要件がない場合には、動作制御部１０１３は、データ処理部７１に対して、文書の読み取りを指示し、ユーザは文書データを取得して終了する。
【０１５１】
一方、キュリティレベルが”high”のときの場合のように、抽出すべき要件がある場合には、動作要件選択部１０１２は、その要件をすべて満たすことができるかを判定し、その判断結果を動作制御部１０１３に通知する。
【０１５２】
動作要件選択部１０１２による判断結果がすべての要件を満たすことができないことを示す場合は、動作制御部１０１３は、データ処理部７４に対してデータ処理を禁止するように指示し、データ処理部７４は読み取りデータを破棄して終了する。ユーザに対してはデータ処理が行えないことを通知する。
【０１５３】
一方、動作要件選択部１０１２による判断結果がすべての要件を満たすことができることを示す場合は、動作制御部１０１３データ処理部７４に対して、その要件を満たすよう

にデータ処理を行うように指示する。ユーザは文書データを取得して終了する。

【０１５４】

この場合には、以下の処理が実行される。

【０１５５】

ユーザ属性取得部１０２１は、オペレーションパネル３６から読み取り指示を出したユーザに、ユーザＩＤの入力要求を出す。ユーザは、オペレーションパネル３６からユーザＩＤを入力する。ユーザ属性取得部１０２１は、ユーザＩＤからデータベース１０２に登録されている入力されたユーザＩＤに対応するカテゴリー、セキュリティレベルを取得し、動作要件選択部１０２１に通知する。

【０１５６】

ログを記録する場合、読み取った文書データに追跡可能な情報の埋め込み(例えば、電子すかしの埋め込み、表示可能なラベルの埋め込み、文書属性情報の追加など)を行う。表示可能なラベルは、読み取りを指示したユーザの認証データと読み取りを指示した時点のタイムスタンプを含んでもよい。

【０１５７】

最後に、ユーザは紙原稿６０の画像データを蓄積データ６２内に取得して終了する。

【０１５８】

以上のように、図２９に示したセキュリティポリシーに従って、紙原稿（ドキュメント）６０を読み取ることができる。

【０１５９】

次に、画像形成装置１０００が紙原稿６０を読み取り且つ読み取った文書をネットワークに配信する場合について説明する。

【０１６０】

先ず、ユーザが、画像形成装置１０００に紙原稿６０をセットし、オペレーションパネル３６から、読み取り条件の入力、読み取りデータの配信先の指定及び紙原稿６０の読み取り指示を出す。

【０１６１】

読み取り部７１が、紙文書の読み取りを行う。ドキュメント属性取得部１０１１は、読み取った紙原稿６０の画像データのバーコードや電子透かしなどの画像情報から文書ＩＤを抽出し、カテゴリー、セキュリティレベルを取得して、動作要件選択部１０１２に通知する。

【０１６２】

動作要件選択部１０１２は、ドキュメント属性取得部１０１１が通知したドキュメント属性に従って、ＤＳＰ２１００の中の対応するエントリを検索し、要件を抽出する。

【０１６３】

上述の図２９に示すＤＳＰ２１００に基づいて、例えば、セキュリティレベルが”basic”の文書を読み取り、ネットワーク配信しようとしている場合には、読み取りに関する要件はない。しかし、上述のように、ネットワークに配信する時には、「ログを記録すること」と「プリント制限をかけること」と「信頼できるチャネルを使用すること」が要件となる。

【０１６４】

また、上述の図２９に示すＤＳＰ２１００に基づいて、例えば、セキュリティレベルが”high”の文書を読み取りしようとしている場合には、読み取りに関する要件として、「ログを記録すること」と「追跡可能な情報を埋め込むこと(例えば、上述のような、電子すかしの埋め込み、表示可能なラベルの埋め込み、文書属性情報の追加など)」が要件となる。しかし、ネットワークに配信することを許可するルールがないため、許可されない。

【０１６５】

例えば、ドキュメントをネットワークへ配信する際の要件が、ＤＳＰ２１００内に存在しない場合には、動作制御部１０１３は、データ送信部７５に対して配信の指示を行い、

ドキュメントをネットワークへ配信して、処理を終了する。

【０１６６】

一方、例えば、ドキュメントをネットワークへ配信する際の要件が、ＤＳＰ２１００内に存在する場合には、動作要件選択部１０１２が、その要件をすべて満たすことができるかを判定する。

【０１６７】

ネットワークに配信することを許可するルールがない場合には、動作制御部１０１３が、ユーザに、「ネットワークに配信することを許可するルールがない」ことを通知をして、紙原稿６０の画像データを破棄して終了する。例えば、セキュリティレベルが”high”の場合である。

【０１６８】

動作要件選択部１０１２によってすべての要件を満たすことができないと判断した場合は、動作制御部１０１３が、ユーザに通知をして、データ処理部７４に対して紙原稿６０の画像データを破棄するように指示して終了する。

【０１６９】

例えば、上述のセキュリティレベルが”basic”の場合のように、すべての要件を満たすことができる場合は、動作制御部１０１３は、その要件を満たした読み取りをデータ処理部７４に指示し、また、データ送信部７５にドキュメントをネットワークに配信するように指示して終了する。

【０１７０】

そして、ユーザ属性取得部１０１２は、オペレーションパネル３６から読み取り指示を出したユーザに、ユーザＩＤの入力要求を出す。

【０１７１】

ユーザが、オペレーションパネル３６からユーザＩＤを入力すると、ユーザ属性取得部１０２１は、ユーザＩＤに対応するカテゴリー、セキュリティレベルを取得し、動作要件選択部１０１２に通知する。動作制御部１０１３は、動作要件選択部１０１２から通知される要件に従ってログを記録する。

【０１７２】

更に、動作制御部１０１３は、データ処理部７４に対して、読み取った紙原稿６０の画像データを、印刷不可能なデータ(たとえばADOBE（登録商標）の印刷禁止属性を持ったPDFなど)に変換するように指示を行う。

【０１７３】

最後に、動作制御部１０１３は、データ送信部７５に対して配信指示を行い、データ送信部７５は、信頼できる通信経路(たとえばIPsecやVPNなど)を通じて、ドキュメントをネットワークへ配信し、終了する。

【０１７４】

以上のように、図２９に示したＤＳＰ２１００を使用して、図２８に示した文書読み取り装置としての画像形成装置１０００が、文書を読み取り且つ読み取った文書をネットワークに配信することができる。

【０１７５】

セキュリティポリシーに従った動作を実現する複写装置としての画像形成装置の機能構成について図３０で説明する。図３０は、セキュリティポリシーに従って動作する複写装置としての画像形成装置の機能構成を示す図である。図３０中、図２８と同様の処理部には同一符号を付しその詳細な説明を省略する。

【０１７６】

図３０において、複写装置としての画像形成装置１０００－２は、図２８に示す画像形成装置１０００の読み取り条件取得部７２及びデータ送信先取得部７３の代わりに複写条件取得部８１と、図２８に示す画像形成装置１０００のデータ送信部７５の代わりに印刷部８２とを有する点において、図２８に示す画像形成装置１０００と異なっている。

【０１７７】

しかしながら、画像形成装置１０００が画像形成装置１０００－２の複写条件取得部８１と、印刷部８２とを更に有するように構成しても良い。点線で示される部分１００２は省略しても良い。

【０１７８】

複写条件取得部８１は、ユーザがオペレーションパネル３６に入力した複写条件を取得して、読み取り部７１とデータ処理部７４とへ複写条件を通知すると共に、印刷部８２へも通知する。

【０１７９】

印刷部８２は、動作制御部１０１３からの指示に応じて、蓄積データ６２から紙原稿６０の画像データを取得し、動作制御部１０１３から通知された要件を満たすように複写条件取得部８１から通知された複写条件に従って印刷処理を行い、用紙に画像データが形成された複写原稿６０ｂを出力する。

【０１８０】

以下に、ドキュメント属性取得部１０１１とユーザ属性取得部１０２１について詳述する。

【０１８１】

図３１は、ドキュメントの識別情報をバーコードで印字した場合を示す図である。図３１に示すドキュメント６１０では、所定位置にバーコード６１１で識別情報が印字されている。この場合、ドキュメント属性取得部１０１１は、図３２に示すように、紙原稿６０としてのドキュメント６１０から直接識別情報を取得し、その識別情報からドキュメント属性を取得するように構成される。

【０１８２】

図３２は、ドキュメント属性取得部の第一機能構成を示す図である。図３２において、ドキュメント属性取得部１０１１－１は、識別情報取得部１０３１と、ドキュメント属性読み取り部１０３２と、ドキュメント属性ＤＢ６４とを有する。

【０１８３】

識別情報取得部１０３１は、紙原稿６０から図３１に示されるドキュメント６１０のバーコード６１１を読み取って、識別情報として取得し、ドキュメント属性読み取り部１０３２に通知する。

【０１８４】

ドキュメント属性読み取り部１０３２は、テーブルＴ１００を参照することによって、識別情報取得部１０３１から通知された識別情報に基づいてドキュメント属性を取得して、動作要件選択部１０１２へ通知する。

【０１８５】

ドキュメント属性ＤＢ１０１１－１は、テーブルＴ１００によってドキュメント属性を管理する。テーブルＴ１００は、識別情報としてドキュメントＩＤ、カテゴリー、レベル、取り扱い可能ゾーン等の項目を有する。ドキュメント属性読み取り部１０３２は、ドキュメント属性として、カテゴリー、レベル、取り扱い可能ゾーン等の情報を取得することができる。

【０１８６】

このような機能構成は、バーコード、ＲＦＩＤ、ＭＣＲ等の専用の読み取り装置が既に利用されている場合に適している。

【０１８７】

図３３は、ドキュメントの識別情報を数字で印字した場合を示す図である。図３３に示すドキュメント６２０では、所定位置に数字６２１で識別情報が印字されている。この場合、ドキュメント属性取得部１０１１は、図３４に示すように、紙原稿６０としてのドキュメント６１０から直接識別情報を取得し、その識別情報からドキュメント属性を取得するように構成される。

【０１８８】

図３４は、ドキュメント属性取得部の第二機能構成を示す図である。図３４中、図３２

と同様の処理部には同一の符号を付し、その説明を省略する。

【０１８９】

図３４において、ドキュメント属性取得部１０１１－２は、識別情報取得部１０３１と、ドキュメント属性読み取り部１０３２と、ドキュメント属性ＤＢ６４とを有する点で図３２に示すドキュメント属性取得部１０１１－１と同様であるが、一旦読み取り部７１によって読み取った紙原稿６０の画像データが格納されている読み取り画像データ６１からその画像データを取り出して、ＯＣＲ等の文字認識機能を利用して識別することによって、ドキュメント属性を取得する点が異なっている。テーブルＴ１００のデータ構成も図３２に示すドキュメント属性取得部１０１１－１と同様である。

【０１９０】

図３５は、ドキュメントの識別情報を前面に印字した場合を示す図である。図３５に示すドキュメント６３０では、前面に識別情報を示すドットパターンが印字されている。

【０１９１】

図３６は、ドキュメントのセキュリティ属性を文字で印字した場合を示す図である。図３６に示すドキュメント６４０は、所定位置に例えばドキュメント属性を示す「秘」６４１が直接印字されている。

【０１９２】

このような場合、読み取り部７１によって取得した画像データをＯＣＲなどで文字認識し、所定位置に印字されているドキュメント属性を取得する。

【０１９３】

図３７は、ドキュメント属性取得部の第三機能構成を示す図である。図３７において、ドキュメント属性取得部１０１１－３は、文字読み取り部１０３５と、カテゴリー辞書６５と、レベル辞書６６と、取り扱いゾーン辞書６７等を夫々管理するデータベースとを有する。

【０１９４】

次に、ユーザ属性取得部１０２１について詳述する。

【０１９５】

図３８は、ユーザ属性取得部の機能構成を示す図である。図３８において、ユーザ属性取得部１０２１は、ユーザ情報取得部１０４１と、ユーザ認証部１０４２と、ユーザ属性読み取り部１０４３と、ユーザ属性ＤＢ６８とを有する。

【０１９６】

ユーザ情報取得部１０４１は、ユーザによってオペレーションパネル３６に入力されたユーザ情報を取得して、ユーザ認証部１０４２に通知する。

【０１９７】

ユーザ認証部１０４２は、ユーザ属性ＤＢ６８を参照することによって、ユーザ情報に基づいて、ユーザ認証を行い、認証が成功した場合にユーザ属性を取得して、ユーザ属性読み取り部１０４３に通知する。

【０１９８】

ユーザ属性ＤＢ６８は、ユーザ情報としてユーザＩＤとパスワードの項目を有し、ユーザ属性としてカテゴリー、レベル等の項目を有するテーブルＴ２００によってユーザ属性を管理する。

【０１９９】

ユーザ属性読み取り部１０４３は、ユーザ属性を動作要件選択部１０１２に通知する。

【０２００】

ドキュメント属性と同様に外部サーバによって実現することも可能である。外部サーバを利用することで、Ｗｉｎｄｏｗｓ（登録商標）、ＬｏｔｕｓＮｏｔｅｓなどを利用するユーザ等との連携が容易に実現可能となる。

【０２０１】

図３９は、ユーザ属性を外部を外部サーバから取得する場合の機能構成を示す図である。図３９中、図３８と同様の処理部には同一の符号を付し、その説明を省略する。図３９

において、ユーザ属性取得部１０１２－２は、ユーザ情報取得部１０４１と通信処理部１０４５とを有する。

【０２０２】

通信処理部１０４５は、外部サーバとしてのユーザ属性サーバ８０へ、ユーザ情報を送信することによってユーザ属性の要求を行い、ユーザ属性サーバ８０から取得したユーザ属性を動作要件選択部１０１２に通知する。

【０２０３】

外部サーバとしてのユーザ属性サーバ８０は、通信処理部８５と、ユーザ認証部８２と、ユーザ属性読み取り部８３と、ユーザ属性ＤＢ６９とを有する。

【０２０４】

通信処理部８５は、ユーザ属性取得部１０２１－２からの要求に応じて、ユーザ情報をユーザ認証部８２に通知する。

【０２０５】

ユーザ認証部８２は、ユーザ属性ＤＢ６８９参照することによって、ユーザ情報に基づいて、ユーザ認証を行い、認証が成功した場合にユーザ属性を取得して、通信処理部８５に通知する。

【０２０６】

通信処理部８５は、ユーザ属性をユーザ属性取得部１０２１－２に通知する。

【０２０７】

上述より、埋め込み情報が文書を一意に識別するバーコード情報、透かし情報、地紋情報のうち少なくとも一つの情報であることにより、埋め込み情報で文書のコンテンツや文書属性を識別して文書に関する処理が実行されるため、文書のセキュリティを確保することができる。

【０２０８】

本発明の一実施例に係る画像形成装置１０００は、プリンタ、ＦＡＸ、コピー等の複数の異なる画像形成機能の少なくとも１つを有する装置である。

【図面の簡単な説明】

【０２０９】

【図１】セキュリティポリシーの例を示す図である。
【図２】ドキュメントラベル用語ファイルのリストの例を示す図である。
【図３】ポリシー用語ファイルの例を示す図である。
【図４】ポリシー用語ファイルの例を示す図である。
【図５】ポリシー用語ファイルの例を示す図である。
【図６】ポリシー用語ファイルの例を示す図である。
【図７】ポリシー用語ファイルの例を示す図である。
【図８】ポリシー用語ファイルの例を示す図である。
【図９】ポリシー用語ファイルの例を示す図である。
【図１０】ポリシー用語ファイルの例を示す図である。
【図１１】ポリシー用語ファイルの例を示す図である。
【図１２】ポリシー用語ファイルの例を示す図である。
【図１３】ポリシー用語ファイルの例を示す図である。
【図１４】ポリシーファイルの例を示す図である。
【図１５】ポリシーファイルの例を示す図である。
【図１６】ポリシーファイルの例を示す図である。
【図１７】ポリシーファイルの例を示す図である。
【図１８】ポリシーファイルの例を示す図である。
【図１９】ポリシーファイルの例を示す図である。
【図２０】ポリシーファイルの例を示す図である。
【図２１】ポリシーファイルの例を示す図である。
【図２２】ポリシーファイルの例を示す図である。

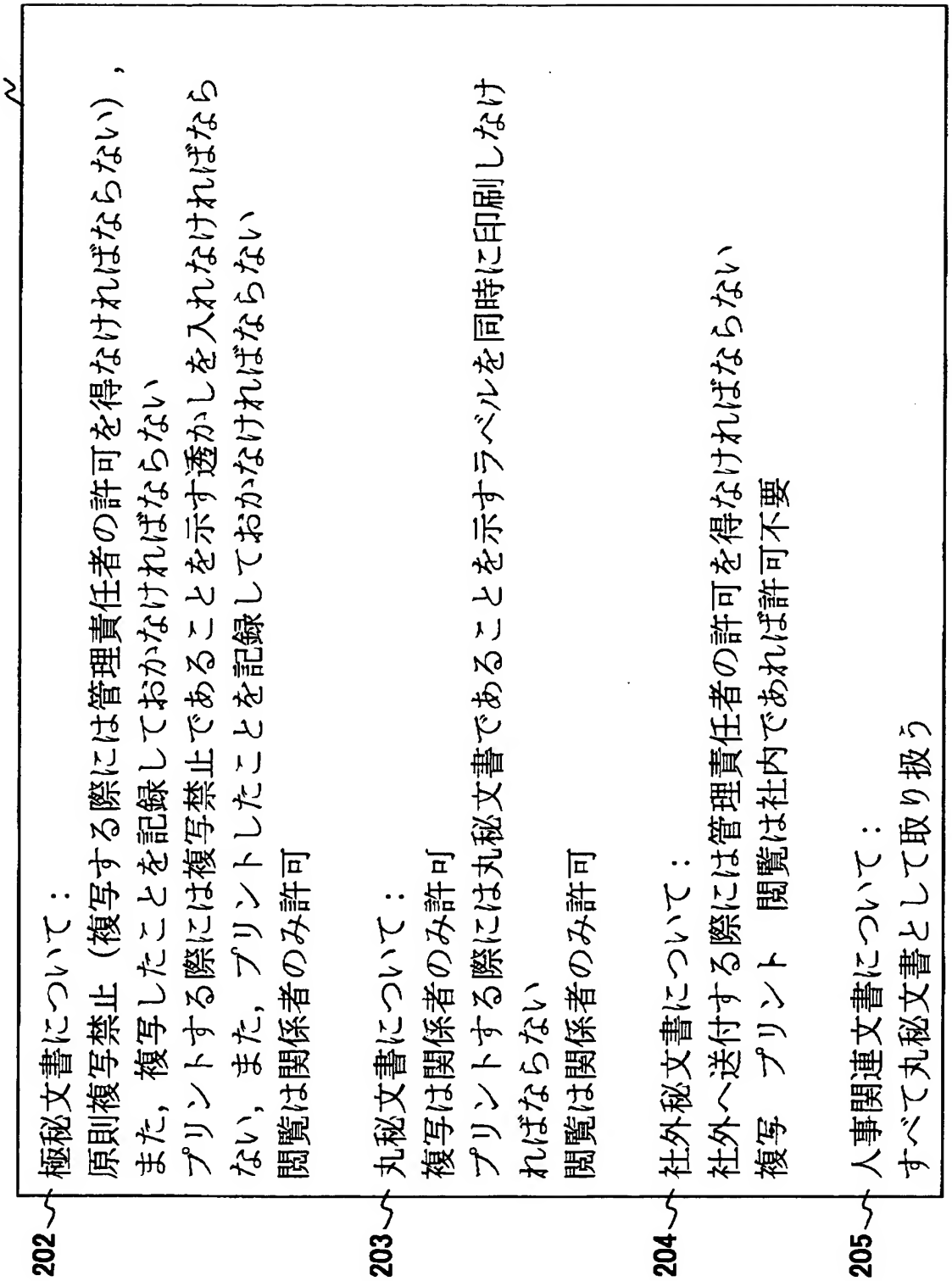
【図２３】ＤＳＰの識別情報の例を示す図である。
【図２４】ＤＳＰの構造を説明するための記述例を示す図である。
【図２５】ＤＳＰの他の記述例を示す図である
【図２６】ＤＳＰを蓄積し且つ配布する種々の媒体を示す図である。
【図２７】本発明の一実施例に係る画像形成装置のハードウェア構成を示すブロック図である。
【図２８】セキュリティポリシーに従って動作する読み取り装置としての画像形成装置の機能構成を示す図である。
【図２９】簡略化したＤＳＰの例を示す図である。
【図３０】セキュリティポリシーに従って動作する複写装置としての画像形成装置の機能構成を示す図である。
【図３１】ドキュメントの識別情報をバーコードで印字した場合を示す図である。
【図３２】ドキュメント属性取得部の第一機能構成を示す図である。
【図３３】ドキュメントの識別情報を数字で印字した場合を示す図である。
【図３４】ドキュメント属性取得部の第二機能構成を示す図である。
【図３５】ドキュメントの識別情報を前面に印字した場合を示す図である。
【図３６】ドキュメントのセキュリティ属性を文字で印字した場合を示す図である。
【図３７】ドキュメント属性取得部の第三機能構成を示す図である。
【図３８】ユーザ属性取得部の機能構成を示す図である。
【図３９】ユーザ属性を外部を外部サーバから取得する場合の機能構成を示す図である。

【符号の説明】
【０２１０】

| | |
|---|---|
| ５１ | ハードディスク |
| ５２ | 光磁気ディスク |
| ５３ | フレキシブルディスク |
| ５４ | 光ディスク |
| ５５ | コンピュータ |
| ５６ | ネットワーク |
| ７１ | 読み取り部 |
| ７２ | 読み取り条件取得部 |
| ７３ | データ送信先取得部 |
| ７４ | データ処理部 |
| １０００ | 画像形成装置 |
| １００１ | ポリシー実行部 |
| １０１１ | ドキュメント属性取得部 |
| １０１２ | 動作要件選択部 |
| １０１３ | 動作制御部 |
| １０２１ | ユーザ属性取得部 |
| ２０００ | ＤＳＰ |

【書類名】図面
【図１】

ドキュメントに関するセキュリティポリシーの例を示す図



【図２】

# ドキュメントラベルファイルの例を示す図

300

```
<?xml version="1.0" encoding="SHIFT-JIS" ?>
<document_label_terminology>
<about_this_terminology>
     <serial_number>RDST0001</serial_number>
     <title>
          DOCUMENT-LABEL-TERMINOLOGY
     </title>
     <version>1.00</version>
     <creation_date>2001/12/21 13:37:18</creation_date>
     <creator>Taro Tokyo</creator>
     <description>sample document-label terminology.</description>
</about_this_terminology>
<enumeration>
312 <enum_id>doc_category</enum_id>
313 <enum_name>Document Category</enum_name>
314 <description>文書カテゴリーの種類</description>
     <item>
315          <name>internal_doc</name>
          <description>社内一般文書</description>
     </item>
311  <item>
316          <name>human_resource_doc</name>
          <description>人事関連文書</description>
     </item>
     <item>
317          <name>technical_doc</name>
          <description>技術関連文書</description>
     </item>
</enumeration>
<enumeration>
322 <enum_id>doc_security_level</enum_id>
323 <enum_name>Document Security Level</enum_name>
324 <description>文書のセキュリティレベルの種類</description>
     <item>
325          <name>basic</name>
          <description>社外秘</description>
     </item>
321  <item>
326          <name>medium</name>
          <description>秘</description>
     </item>
     <item>
327          <name>high</name>
          <description>極秘</description>
     </item>
</enumeration>
</document_label_terminology>
```

【図３】

# ポリシー用語ファイルの例を示す図

400

```
<?xml version="1.0" encoding="SHIFT-JIS" ?>
<policy_terminology>
<about_this_terminology>
      <serial_number>RDST9487</serial_number>
      <title>DOCUMENT-SECURITY-POLICY-TERMINOLOGY</title>
      <version>1.00</version>
      <creation_date>2001/12/21 13:37:18</creation_date>
      <creator>Taro Tokyo</creator>
      <description>sample policy terminology.</description>
</about_this_terminology>

<!-- システムタイプの列挙 -->
<enumeration>
      <enum_id>system_type</enum_id>
      <enum_name>System Type</enum_name>
      <description>システムタイプの種類</description>
      <item>
            <name>Copier</name>
            <description>複写機</description>
            <operation>copier_operation</operation>
      </item>
      <item>
            <name>Printer</name>
            <description>プリンタ</description>
            <operation>printer_operation</operation>
      </item>
      <item>
            <name>Facsimile</name>
            <description>ファクシミリ</description>
            <operation>fax_operation</operation>
      </item>
      <item>
            <name>Scanner</name>
            <description>スキャナ</description>
            <operation>scanner_operation</operation>
      </item>
      <item>
            <name>Document Repository</name>
            <description>文書リポジトリ</description>
            <operation>repository_operation</operation>
      </item>
      <item>
            <name>E-Meeting</name>
            <description>電子会議システム</description>
            <operation>emeeting_operation</operation>
      </item>
</enumeration>
```

411

【図４】

# ポリシー用語ファイルの例を示す図

400

```
<!-- システムタイプごとのオペレーションの列挙 -->
<enumeration>
      <enum_id>copier_operation</enum_id>
      <enum_name>Copier Operation</enum_name>
      <description>複写機に関わるオペレーション</description>
      <item>
            <name>hardcopy</name>
            <description>紙から紙への複写</description>
            <requirement>hardcopy_requirement</requirement>
      </item>
</enumeration>
<enumeration>
      <enum_id>printer_operation</enum_id>
      <enum_name>Printer Operation</enum_name>
      <description>プリンタに関わるオペレーション</description>
      <item>
            <name>print</name>
            <description>電子文書を紙へ印刷</description>
            <requirement>print_requirement</requirement>
      </item>
</enumeration>
<enumeration>
      <enum_id>fax_operation</enum_id>
      <enum_name>Facsimile Operation</enum_name>
      <description>ファックスに関わるオペレーション</description>
      <item>
            <name>fax_send</name>
            <description>ファックスの送信</description>
            <requirement>fax_send_requirement</requirement>
      </item>
      <item>
            <name>fax_receive</name>
            <description>ファックスの受信</description>
            <requirement>fax_receive_requirement</requirement>
      </item>
</enumeration>
<enumeration>
      <enum_id>scanner_operation</enum_id>
      <enum_name>Scanner Operation</enum_name>
      <description>スキャナに関わるオペレーション</description>
      <item>
            <name>scan</name>
            <description>紙文書をスキャンして電子文書にする</description>
            <requirement>scan_requirement</requirement>
      </item>
</enumeration>
```

421　431　441　451

【図５】

# ポリシー用語ファイルの例を示す図

400

```
<enumeration>
      <enum_id>repository_operation</enum_id>
      <enum_name>Document Repository Operation</enum_name>
      <description>文書リポジトリに関わるオペレーション</description>
      <item>
            <name>store</name>
            <description>保存する</description>
            <requirement>store_requirement</requirement>
      </item>
      <item>
            <name>revise</name>
            <description>改訂・編集する</description>
            <requirement>revise_requirement</requirement>
      </item>
      <item>
            <name>delete</name>
            <description>削除・破棄する</description>
            <requirement>delete_requirement</requirement>
      </item>
      <item>
            <name>read</name>
            <description>参照する</description>
            <requirement>read_requirement</requirement>
      </item>
      <item>
            <name>net_delivery</name>
            <description>
             ネットワークで配布する（送信する）
            </description>
      <requirement>net_delivery_requirement</requirement>
      </item>
      <item>
            <name>disc_delivery</name>
            <description>ディスクで配布する（送付する）</description>
            <requirement>disc_delivery_requirement</requirement>
      </item>
      <item>
            <name>archive</name>
            <description>アーカイブ・バックアップする</description>
            <requirement>archive_requirement</requirement>
      </item>
</enumeration>
<enumeration>
      <enum_id>emeeting_operation</enum_id>
      <enum_name>E-Meeting Operation</enum_name>
      <description>電子会議システムに関わるオペレーション</description>
 <item>
            <name>meeting_use</name>
            <description>会議で利用する</description>
            <requirement>meeting_use_requirement</requirement>
     </item>
</enumeration>
```

461

471

【図６】

# ポリシー用語ファイルの例を示す図

400

```
<!-- オペレーションごとに適用できる要件の列挙 -->
<!-- ユーザ認証，文書識別，アクセス制御（利用制限）は基本メカニズムとして提供されるため
，要件には含めない -->
<enumeration>
      <enum_id>hardcopy_requirement</enum_id>
      <enum_name>Hardcopy Requirement</enum_name>
      <description>複写に関わる要件</description>
      <item>
            <name>explicit_authorization</name>
            <description>明示的な許可</description>
      </item>
481   <item>
            <name>audit</name>
            <description>監査証跡の記録</description>
      </item>
      <item>
            <name>audit_with_image</name>
            <description>監査証跡のイメージ付き記録</description>
      </item>
</enumeration>
<enumeration>
      <enum_id>print_requirement</enum_id>
      <enum_name>Print Requirement</enum_name>
      <description>印刷に関わる要件</description>
      <item>
            <name>explicit_authorization</name>
            <description>明示的な許可（利用制限）</description>
      </item>
      <item>
            <name>audit</name>
            <description>監査証跡の記録</description>
      </item>
      <item>
            <name>audit_with_image</name>
            <description>監査証跡のイメージ付き記録</description>
      </item>
491   <item>
            <name>private_access</name>
            <description>プリントした本人による紙出力</description>
      </item>
 <item>
            <name>trusted_channel</name>
            <description>
             信頼チャネルの利用（印刷データの暗号化）
            </description>
      </item>
      <item>
            <name>embed_trace_info</name>
            <description>
             プリントアウトに追跡情報埋め込み（透かし，ラベル，バーコード）
            </description>
      </item>
</enumeration>
```

【図７】

# ポリシー用語ファイルの例を示す図

400

```
<enumeration>
      <enum_id>fax_send_requirement</enum_id>
      <enum_name>Requirement on Sending Fax Message</enum_name>
      <description>ファクス送信に関わる要件</description>
      <item>
            <name>explicit_authorization</name>
            <description>明示的な許可（利用制限）</description>
      </item>
      <item>
            <name>audit</name>
            <description>監査証跡の記録</description>
      </item>
      <item>
            <name>audit_with_image</name>
            <description>監査証跡のイメージ付き記録</description>
      </item>
      <item>
            <name>destination_restriction</name>
            <description>宛先制限</description>
      </item>
501   <item>
            <name>private_mode</name>
            <description>親展モードでの送信</description>
      </item>
      <item>
            <name>trusted_channel</name>
            <description>
                  信頼チャネルの利用（ファクスデータの暗号化）
            </description>
      </item>
      <item>
            <name>embed_trace_info</name>
            <description>
                  送信ファクスに追跡情報埋め込み（透かし，ラベル，バーコード）
            </description>
      </item>
      <item>
            <name>non_repudiation</name>
            <description>否認防止（受取証の取得）</description>
      </item>
</enumeration>
```

【図８】

# ポリシー用語ファイルの例を示す図

400

```
<enumeration>
      <enum_id>fax_receive_requirement</enum_id>
      <enum_name>Requirement on Receiving Fax Message</enum_name>
      <description>ファックス受信に関わる要件</description>
      <item>
            <name>audit</name>
            <description>監査証跡の記録</description>
      </item>
      <item>
            <name>audit_with_image</name>
            <description>監査証跡のイメージ付き記録</description>
      </item>
      <item>
            <name>private_access</name>
            <description>親展ファックスの宛先本人による取り出し</description>
      </item>
      <item>
            <name>trusted_timestamp</name>
            <description>信頼タイムスタンプ</description>
      </item>
      <item>
            <name>embed_trace_info</name>
            <description>
             受信ファックスに追跡情報埋め込み（透かし，ラベル，バーコード）
            </description>
      </item>
</enumeration>
<enumeration>
      <enum_id>scan_requirement</enum_id>
      <enum_name>Scan Requirement</enum_name>
      <description>スキャンに関わる要件（保存した後については保存要件を適用する）
      </description>
      <item>
            <name>explicit_authorization</name>
            <description>明示的な許可（利用制限）</description>
      </item>
      <item>
            <name>audit</name>
            <description>監査証跡の記録</description>
      </item>
      <item>
            <name>audit_with_image</name>
            <description>監査証跡のイメージ付き記録</description>
      </item>
      <item>
            <name>embed_trace_info</name>
            <description>
             スキャン画像に追跡情報埋め込み（透かし，ラベル，バーコード）
            </description>
      </item>
</enumeration>
```

511

521

【図９】

# ポリシー用語ファイルの例を示す図

400

```
<enumeration>
      <enum_id>store_requirement</enum_id>
      <enum_name>Store Requirement</enum_name>
      <description>保存に関わる要件</description>
      <item>
            <name>explicit_authorization</name>
            <description>明示的な許可（利用制限）</description>
      </item>
      <item>
            <name>audit</name>
            <description>監査証跡の記録</description>
      </item>
      <item>
            <name>encryption</name>
            <description>保存データの暗号化</description>
      </item>
      <item>
            <name>integrity_protection</name>
            <description>保存データの改ざん保護</description>
      </item>
</enumeration>
<enumeration>
      <enum_id>revise_requirement</enum_id>
      <enum_name>Revise Requirement</enum_name>
      <description>改訂に関わる要件</description>
      <item>
            <name>explicit_authorization</name>
            <description>明示的な許可（利用制限）</description>
      </item>
      <item>
            <name>audit</name>
            <description>監査証跡の記録</description>
      </item>
      <item>
            <name>versioning</name>
            <description>バージョン管理</description>
      </item>
</enumeration>
```

531

541

【図１０】

# ポリシー用語ファイルの例を示す図

400

```
<enumeration>
      <enum_id>delete_requirement</enum_id>
      <enum_name>Delete Requirement</enum_name>
      <description>削除・破棄に関わる要件</description>
      <item>
            <name>explicit_authorization</name>
            <description>明示的な許可（利用制限）</description>
      </item>
      <item>
            <name>audit</name>
            <description>監査証跡の記録</description>
      </item>
      <item>
            <name>audit_with_image</name>
            <description>監査証跡のイメージ付き記録</description>
      </item>
      <item>
            <name>complete_erase</name>
            <description>完全消去</description>
      </item>
</enumeration>
<enumeration>
      <enum_id>read_requirement</enum_id>
      <enum_name>Read Requirement</enum_name>
      <description>参照に関わる要件</description>
      <item>
            <name>explicit_authorization</name>
            <description>明示的な許可（利用制限）</description>
      </item>
      <item>
            <name>audit</name>
            <description>監査証跡の記録</description>
      </item>
      <item>
            <name>edit_restriction</name>
            <description>編集禁止のデータのみ参照許可</description>
      </item>
      <item>
            <name>print_restriction</name>
            <description>印刷禁止のデータのみ参照許可</description>
      </item>
      <item>
            <name>location_restriction</name>
            <description>参照場所限定のデータのみ参照許可</description>
      </item>
      <item>
            <name>user_restriction</name>
            <description>ユーザ限定のデータのみ参照許可</description>
      </item>
</enumeration>
```

551

561

【図１１】

# ポリシー用語ファイルの例を示す図

400

```
<enumeration>
      <enum_id>net_delivery_requirement</enum_id>
      <enum_name>Delivery via Network Requirement</enum_name>
      <description>ネットワーク配信（送信）に関わる要件</description>
      <item>
            <name>explicit_authorization</name>
            <description>明示的な許可（利用制限）</description>
      </item>
      <item>
            <name>audit</name>
            <description>監査証跡の記録</description>
      </item>
      <item>
            <name>audit_with_image</name>
            <description>監査証跡のイメージ付き記録</description>
      </item>
      <item>
            <name>trusted_channel</name>
            <description>信頼チャネルの利用（送信データの暗号化）
</description>
      </item>
571   <item>
            <name>destination_restriction</name>
            <description>宛先制限（社内のみ配信可能など）</description>
      </item>
      <item>
            <name>edit_restriction</name>
            <description>編集禁止のデータのみ配信許可</description>
      </item>
      <item>
            <name>print_restriction</name>
            <description>印刷禁止のデータのみ配信許可</description>
      </item>
      <item>
            <name>location_restriction</name>
            <description>参照場所限定のデータのみ配信許可</description>
      </item>
      <item>
            <name>user_restriction</name>
            <description>ユーザ限定のデータのみ配信許可</description>
      </item>
</enumeration>
```

【図１２】

# ポリシー用語ファイルの例を示す図

400

```
<enumeration>
      <enum_id>disc_delivery_requirement</enum_id>
      <enum_name>Delivery via Disc Requirement</enum_name>
      <description>ディスク配布（送付）に関わる要件</description>
      <item>
            <name>explicit_authorization</name>
            <description>明示的な許可（利用制限）</description>
      </item>
      <item>
            <name>audit</name>
            <description>監査証跡の記録</description>
      </item>
      <item>
            <name>audit_with_image</name>
            <description>監査証跡のイメージ付き記録</description>
      </item>
      <item>
            <name>encryption</name>
            <description>送付データの暗号化</description>
      </item>
      <item>
            <name>integrity_protection</name>
            <description>送付データの改ざん保護</description>
      </item>
      <item>
            <name>edit_restriction</name>
            <description>編集禁止のデータのみ送付許可</description>
      </item>
      <item>
            <name>print_restriction</name>
            <description>印刷禁止のデータのみ送付許可</description>
      </item>
      <item>
            <name>location_restriction</name>
            <description>参照場所限定のデータのみ送付許可</description>
      </item>
      <item>
            <name>user_restriction</name>
            <description>ユーザ限定のデータのみ送付許可</description>
      </item>
</enumeration>
```

581

【図１３】

# ポリシー用語ファイルの例を示す図

400

```
<enumeration>
      <enum_id>archive_requirement</enum_id>
      <enum_name>Archive Requirement</enum_name>
      <description>アーカイブ・バックアップに関わる要件</description>
      <item>
            <name>explicit_authorization</name>
            <description>明示的な許可（利用制限）</description>
      </item>
      <item>
            <name>audit</name>
            <description>監査証跡の記録</description>
      </item>
      <item>
            <name>encryption</name>
            <description>アーカイブデータの暗号化</description>
      </item>
      <item>
            <name>integrity_protection</name>
            <description>アーカイブデータの改ざん保護</description>
      </item>
</enumeration>
<enumeration>
      <enum_id>meeting_use_requirement</enum_id>
      <enum_name>Meeting-use Requirement</enum_name>
      <description>会議での利用に関わる要件</description>
      <item>
            <name>explicit_authorization</name>
            <description>明示的な許可（利用制限）</description>
      </item>
      <item>
            <name>audit</name>
            <description>監査証跡の記録</description>
      </item>
      <item>
            <name>audit_with_image</name>
            <description>監査証跡のイメージ付き記録</description>
      </item>
</enumeration>
</policy_terminology>
```

591

601

【図１４】

# ポリシーファイルの例を示す図

2000

```
<?xml version="1.0" encoding="SHIFT-JIS" ?>
<document_security_policy>
<about_this_policy>
     <serial_number>RDSP2023</serial_number>
     <terminology_applied>RDST9487</terminology_applied>
     <title>DOCUMENT-SECURITY-POLICY</title>
     <version>1.30</version>
     <creation_date>2002/02/18 22:30:24</creation_date>
     <creator>Taro Tokyo</creator>
     <description>sample document security policy.</description>
</about_this_policy>
<policy>                                                    2001
     <acc_rule>                                             2011
          <doc_category>ANY</doc_category>                  2013
          <doc_security_level>basic</doc_security_level>    2013
          <acl>
               <ace>
                    <user_category>ANY</user_category>      2017
                    <user_security_level>ANY</user_security_level>  2017
                    <operation>
                         <name>hardcopy</name>
                         <allowed/><!-- allowed without any requirement -->
                    </operation>
                    <operation>
                         <name>print</name>
                         <allowed/><!-- allowed without any requirement -->
                    </operation>
                    <operation>
                         <name>fax_send</name>
                         <requirement>audit</requirement>
                         <requirement>explicit_authorization</requirement>
                    </operation>
                    <operation>
                         <name>fax_receive</name>
                         <allowed/><!-- allowed without any requirement -->
                    </operation>
                    <operation>
                         <name>scan</name>
                         <allowed/><!-- allowed without any requirement -->
                    </operation>
```

【図１５】

# ポリシーファイルの例を示す図

2000

```
                <operation>
                    <name>store</name>
                    <allowed/><!-- allowed without any requirement -->
                </operation>
                <operation>
                    <name>revise</name>
                    <allowed/><!-- allowed without any requirement -->
                </operation>
                <operation>
                    <name>delete</name>
                    <allowed/><!-- allowed without any requirement -->
                </operation>
                <operation>
                    <name>read</name>
                    <allowed/><!-- allowed without any requirement -->
                </operation>
                <operation>
                    <name>net_delivery</name>
                    <requirement>audit</requirement>
                    <requirement>explicit_authorization</requirement>
                    <requirement>print_restriction</requirement>
                    <requirement>trusted_channel</requirement>
                </operation>
                <operation>
                    <name>disc_delivery</name>
                    <requirement>audit</requirement>
                    <requirement>explicit_authorization</requirement>
                    <requirement>print_restriction</requirement>
                </operation>
                <operation>
                    <name>archive</name>
                    <allowed/><!-- allowed without any requirement -->
                </operation>
                <operation>
                    <name>meeting_use</name>
                    <allowed/><!-- allowed without any requirement -->
                </operation>
            </ace>
        </acl>
    </acc_rule>
```

2012

【図１６】

# ポリシーファイルの例を示す図

2000

```
<acc_rule>                                          2021
2023 { <doc_category>ANY</doc_category>
       <doc_security_level>medium</doc_security_level>
       <acl>
            <ace>
       2027 { <user_category>DOC-CATEGORY</user_category>
              <user_security_level>ANY</user_security_level>
              <operation>
                   <name>hardcopy</name>
                   <requirement>audit</requirement>
                   <requirement>embed_trace_info</requirement>
              </operation>
              <operation>
                   <name>print</name>
                   <requirement>audit</requirement>
                   <requirement>embed_trace_info</requirement>
              </operation>
              <operation>
                   <name>fax_send</name>
                   <denied/>
                   <!— denied even if it is explicitly authorized -->
              </operation>
              <operation>
                   <name>fax_receive</name>
                   <allowed/><!-- allowed without any requirement —>
              </operation>
              <operation>
                   <name>scan</name>
                   <requirement>audit</requirement>
                   <requirement>embed_trace_info</requirement>
              </operation>
              <operation>
                   <name>store</name>
                   <allowed/><!-- allowed without any requirement -->
              </operation>
```

【図１７】

# ポリシーファイルの例を示す図

2000

```
        <operation>
            <name>revise</name>
            <allowed/><!-- allowed without any requirement -->
        </operation>
        <operation>
            <name>delete</name>
            <allowed/><!-- allowed without any requirement -->
        </operation>
        <operation>
            <name>read</name>
            <requirement>audit</requirement>
            <requirement>print_restriction</requirement>
            <requirement>location_restriction</requirement>
        </operation>
        <operation>
            <name>net_delivery</name>
            <requirement>audit</requirement>
            <requirement>explicit_authorization</requirement>
            <requirement>print_restriction</requirement>
            <requirement>trusted_channel</requirement>
        </operation>
        <operation>
            <name>disc_delivery</name>
            <requirement>audit</requirement>
            <requirement>explicit_authorization</requirement>
            <requirement>print_restriction</requirement>
        </operation>
        <operation>
            <name>archive</name>
            <allowed/><!-- allowed without any requirement -->
        </operation>
        <operation>
            <name>meeting_use</name>
            <allowed/><!-- allowed without any requirement -->
        </operation>
    </ace>
```

【図１８】

# ポリシーファイルの例を示す図

2000

```
<ace>
2028 <user_category>ANY</user_category>
     <user_security_level>ANY</user_security_level>
     <operation>
          <name>hardcopy</name>
          <denied/>
          <!-- denied even if it is explicitly authorized -->
     </operation>
     <operation>
          <name>print</name>
          <denied/>
          <!-- denied even if it is explicitly authorized -->
     </operation>
     <operation>
          <name>fax_send</name>
          <denied/>
          <!-- denied even if it is explicitly authorized -->
     </operation>
     <operation>
          <name>fax_receive</name>
          <denied/>
          <!-- denied even if it is explicitly authorized -->
     </operation>
     <operation>
          <name>scan</name>
          <denied/>
          <!-- denied even if it is explicitly authorized -->
     </operation>
     <operation>
          <name>store</name>
          <denied/>
          <!-- denied even if it is explicitly authorized -->
     </operation>
     <operation>
          <name>revise</name>
          <denied/>
          <!-- denied even if it is explicitly authorized -->
     </operation>
     <operation>
          <name>delete</name>
          <denied/>
          <!-- denied even if it is explicitly authorized -->
     </operation>
```

【図１９】

# ポリシーファイルの例を示す図

2000

```
                <operation>
                    <name>read</name>
                    <requirement>explicit_authorization</requirement>
                    <requirement>audit</requirement>
                    <requirement>print_restriction</requirement>
                    <requirement>location_restriction</requirement>
                </operation>
                <operation>
                    <name>net_delivery</name>
                    <denied/>
                    <!-- denied even if it is explicitly authorized -->
                </operation>
                <operation>
                    <name>disc_delivery</name>
                    <denied/>
                    <!-- denied even if it is explicitly authorized -->
                </operation>
                <operation>
                    <name>archive</name>
                    <denied/>
                    <!-- denied even if it is explicitly authorized -->
                </operation>
                <operation>
                    <name>meeting_use</name>
                    <denied/>
                    <!   denied even if it is explicitly authorized   >
                </operation>
            </ace>
        </acl>
    </acc_rule>~~2022
    <acc_rule>~~2031
2033{   <doc_category>ANY</doc_category>
2033{   <doc_security_level>high</doc_security_level>
        <acl>
            <ace>
2037{           <user_category>DOC-CATEGORY</user_category>
2037{           <user_security_level>ANY</user_security_level>
                <operation>
                    <name>hardcopy</name>
                    <denied/>
                    <!-- denied even if it is explicitly authorized -->
                </operation>
                <operation>
                    <name>print</name>
                    <requirement>explicit_authorization</requirement>
                    <requirement>audit</requirement>
                    <requirement>private_access</requirement>
                    <requirement>trusted_channel</requirement>
                    <requirement>embed_trace_info</requirement>
                </operation>
```

【図２０】

# ポリシーファイルの例を示す図

2000

```
<operation>
     <name>fax_send</name>
     <denied/>
     <!-- denied even if it is explicitly authorized -->
</operation>
<operation>
     <name>fax_receive</name>
     <allowed/><!-- allowed without any requirement -->
</operation>
<operation>
     <name>scan</name>
     <denied/>
     <!-- denied even if it is explicitly authorized -->
</operation>
<operation>
     <name>store</name>
     <requirement>audit</requirement>
     <requirement>encryption</requirement>
     <requirement>integrity_protection</requirement>
</operation>
<operation>
     <name>revise</name>
     <requirement>versioning</requirement>
</operation>
<operation>
     <name>delete</name>
     <requirement>complete_erase</requirement>
</operation>
<operation>
     <name>read</name>
     <requirement>audit</requirement>
     <requirement>print_restriction</requirement>
     <requirement>location_restriction</requirement>
     <requirement>user_restriction</requirement>
</operation>
<operation>
     <name>net_delivery</name>
     <denied/>
     <!-- denied even if it is explicitly authorized -->
</operation>
```

【図２１】

# ポリシーファイルの例を示す図

2000

```
        <operation>
            <name>disc_delivery</name>
            <requirement>audit</requirement>
            <requirement>explicit_authorization</requirement>
            <requirement>encryption</requirement>
            <requirement>print_restriction</requirement>
        </operation>
        <operation>
            <name>archive</name>
            <requirement>encryption</requirement>
            <requirement>integrity_protection</requirement>
        </operation>
        <operation>
            <name>meeting_use</name>
            <requirement>explicit_authorization</requirement>
        </operation>
    </ace>
    <ace>
2038{   <user_category>ANY</user_category>
    <user_security_level>ANY</user_security_level>
        <operation>
            <name>hardcopy</name>
            <denied/>
            <!-- denied even if it is explicitly authorized -->
        </operation>
        <operation>
            <name>print</name>
            <denied/>
            <!-- denied even if it is explicitly authorized -->
        </operation>
        <operation>
            <name>fax_send</name>
            <denied/>
            <!-- denied even if it is explicitly authorized -->
        </operation>
        <operation>
            <name>fax_receive</name>
            <denied/>
            <!-- denied even if it is explicitly authorized -->
        </operation>
        <operation>
            <name>scan</name>
            <denied/>
            <!-- denied even if it is explicitly authorized -->
        </operation>
```

【図２２】

# ポリシーファイルの例を示す図

2000

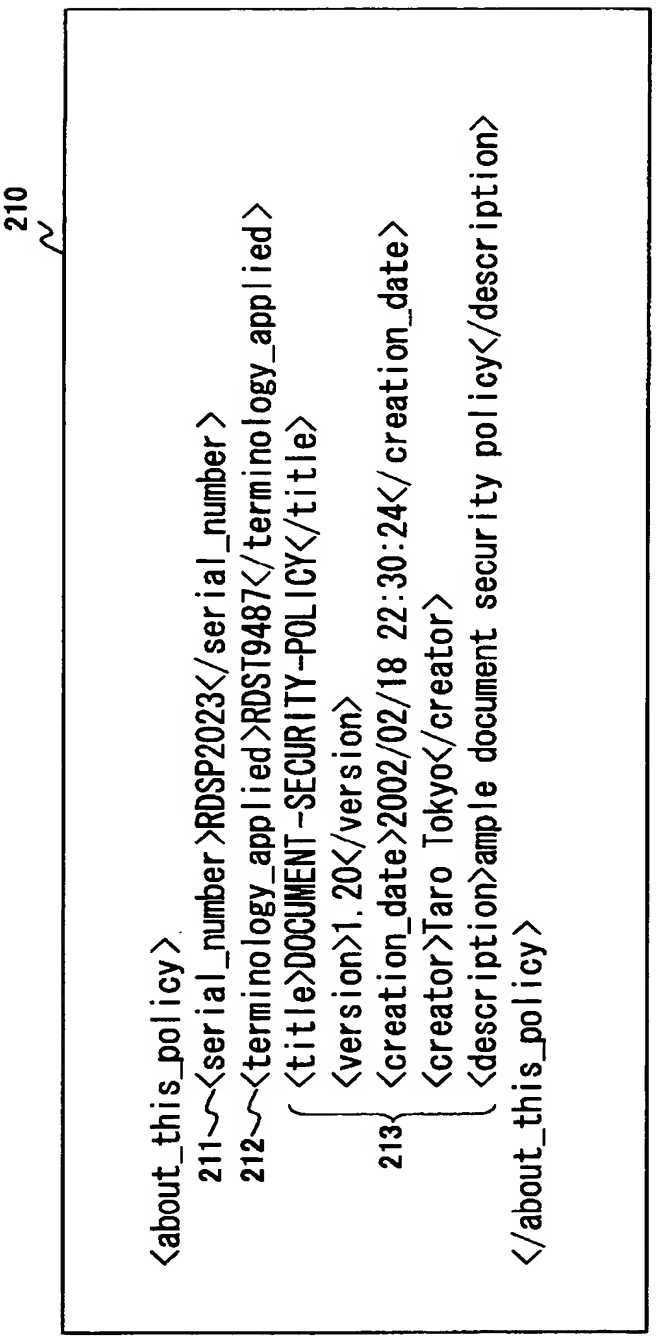
```
                <operation>
                    <name>store</name>
                    <denied/>
                    <!-- denied even if it is explicitly authorized -->
                </operation>
                <operation>
                    <name>revise</name>
                    <denied/>
                    <!-- denied even if it is explicitly authorized -->
                </operation>
                <operation>
                    <name>delete</name>
                    <denied/>
                    <!-- denied even if it is explicitly authorized -->
                </operation>
                <operation>
                    <name>read</name>
                    <requirement>explicit_authorization</requirement>
                    <requirement>audit</requirement>
                    <requirement>print_restriction</requirement>
                    <requirement>location_restriction</requirement>
                    <requirement>user_restriction</requirement>
                </operation>
                <operation>
                    <name>net_delivery</name>
                    <denied/>
                    <!-- denied even if it is explicitly authorized -->
                </operation>
                <operation>
                    <name>disc_delivery</name>
                    <denied/>
                    <!-- denied even if it is explicitly authorized -->
                </operation>
                <operation>
                    <name>archive</name>
                    <denied/>
                    <!-- denied even if it is explicitly authorized -->
                </operation>
                <operation>
                    <name>meeting_use</name>
                    <denied/>
                    <!-- denied even if it is explicitly authorized -->
                </operation>
            </ace>
        </acl>
    </acc_rule>
</policy>
</document_security_policy>
```

2032

2002

【図２３】

DSPの識別情報を示す図



【図２４】

# DSPの構造を説明するための記述例を示す図

220

```
<policy>
221 <acc_rule>
      232 <doc_category>ANY</doc_category>
          <doc_security_level>medium</doc_security_level>
    223 <acl>
          224 <ace>
                225 <user_category>DOC-CATEGORY
                    </user_category>
                226 <user_security_level>ANY
                    </user_security_level>
                227 <operation>
                      228 <name>fax_send</name>
                      229 <denied/><!-- denied even if it
                            is explicitly authorized -->
                    </operation>
                227 <operation>
                      <name>net_delivery</name>
                      230 <requirement>audit
                      </requirement>
                      231 <requirement>
                            explicit_authorization
                      </requirement>
                      …
                    </operation>
                227 <operation>
                      <name>fax_receive</name>
                      232 <allowed/><!-allowed
                        without requirements -->
                    </operation>
                    …
                </ace>
                <ace>
                    …
                </ace>
          </acl>
    </acc_rule>
221 <acc_rule>
          <doc_category>ANY</doc_category>
          <doc_security_level>high</doc_security_level>
          <acl>
              …
          </acl>
    </acc_rule>
</policy>
```

【図２５】

# DSPの他の記述例を示す図

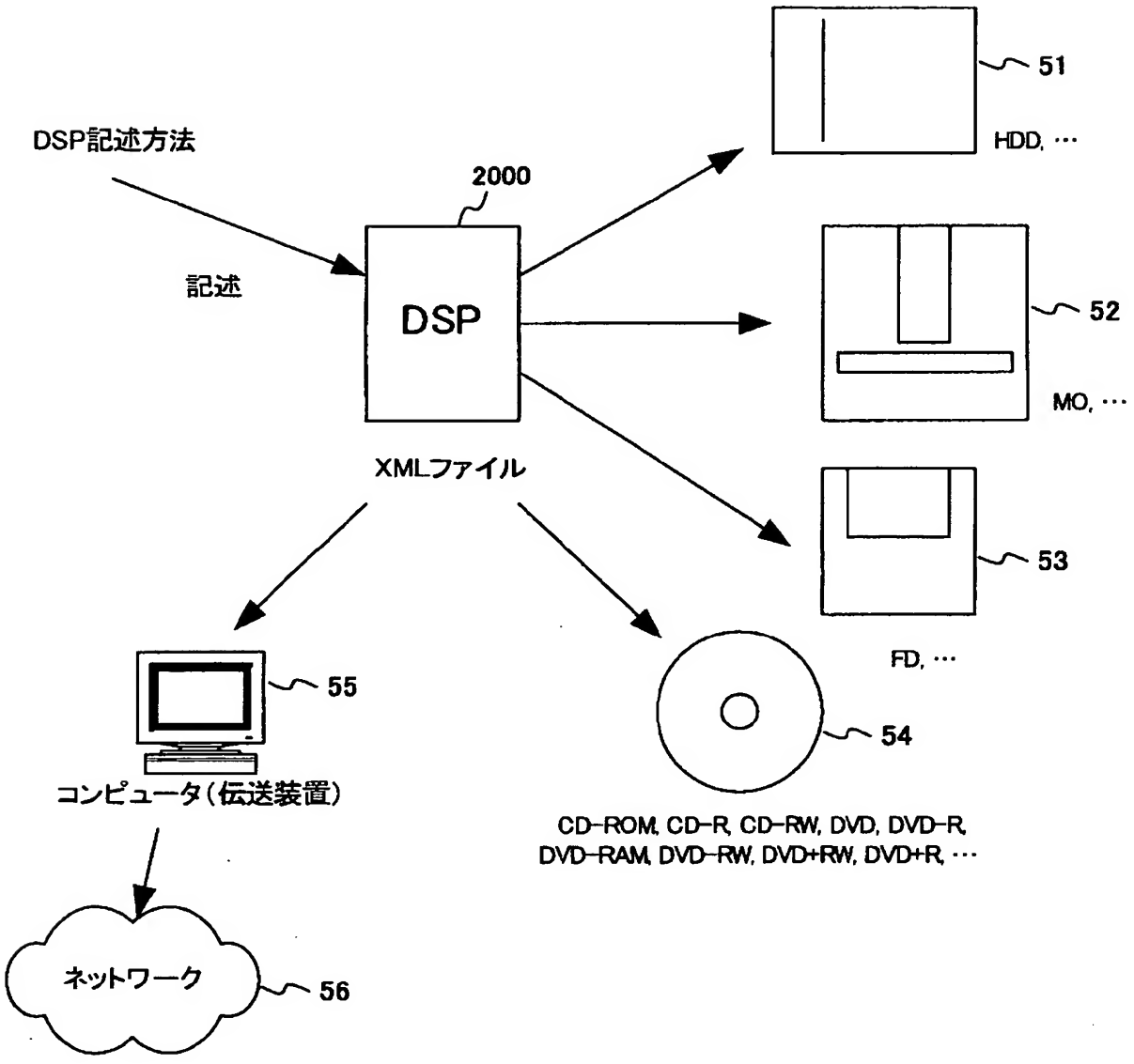
240

```
<policy>
    <acc_rule>
        <doc_category>ANY</doc_category>
        <doc_security_level>medium</doc_security_level>
        <acl>
            <ace>
                <user_category>DOC-CATEGORY</user_category>

<user_security_level>ANY</user_security_level>
241~~<denied_operations>
                <!-- denied even if it is explicitly
                 authorized -->
                    <name>fax_send</name>
                </denied_operations>
                <operation>
                    <name>net_delivery</name>
                    <requirement>audit</requirement>
242~~<requirement>explicit_authorization
                    </requirement>
                                ...
                </operation>
                <operation>
                                ...
                </operation>
243~~<allowed_operations> <!-- allowed without
                                requirements -->
                    <name>fax_receive</name>
                    <name>store</name>
                                ...
                </allowed_operations>
            </ace>
            <ace>
                        ...
            </ace>
                        ...
        </acl>
    </acc_rule>
    <acc_rule>
        <doc_category>ANY</doc_category>
        <doc_security_level>high</doc_security_level>
        <acl>
                        ...
        </acl>
    </acc_rule>
</policy>
```

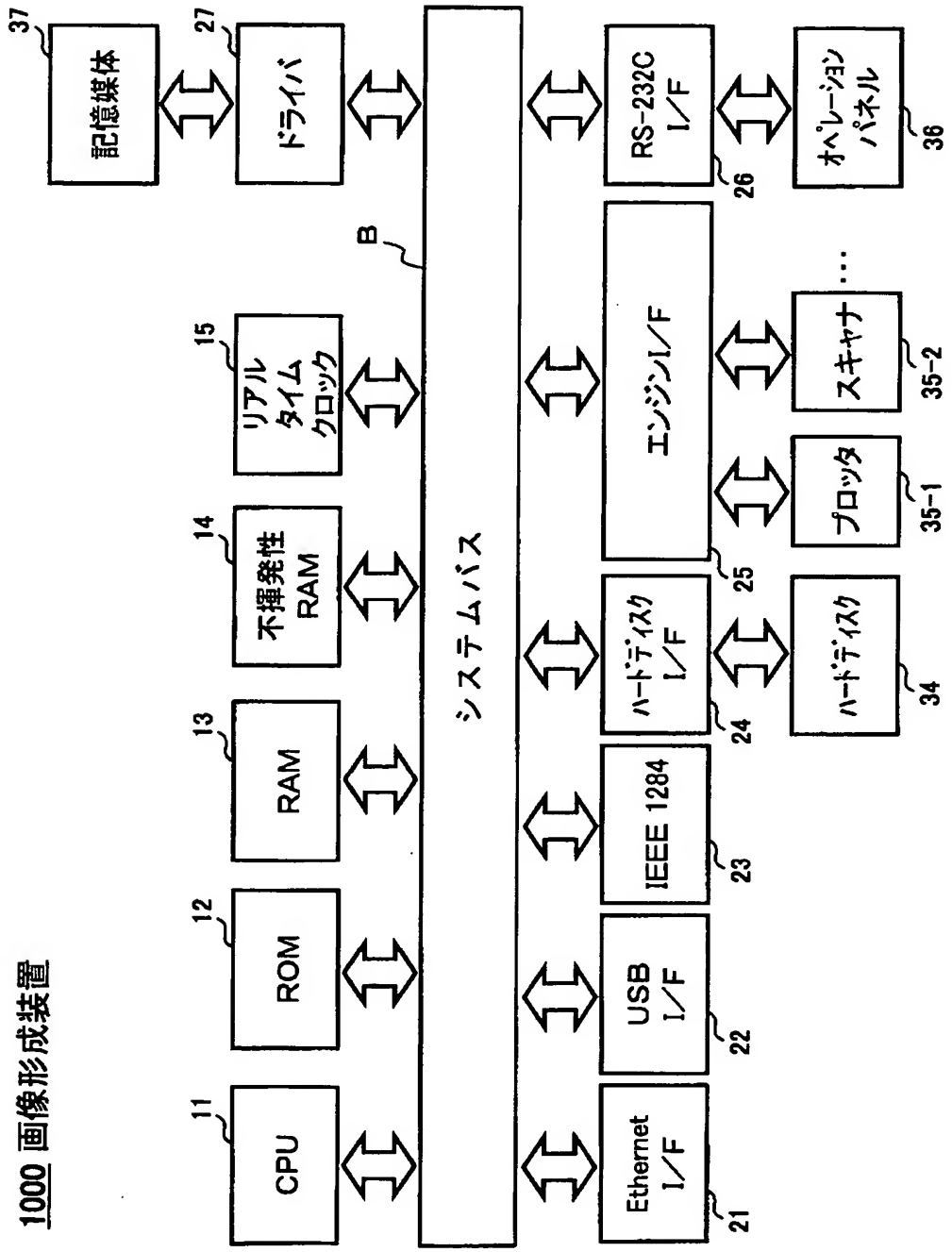
【図２６】

DSPを蓄積し且つ配布する種々の媒体を示す図



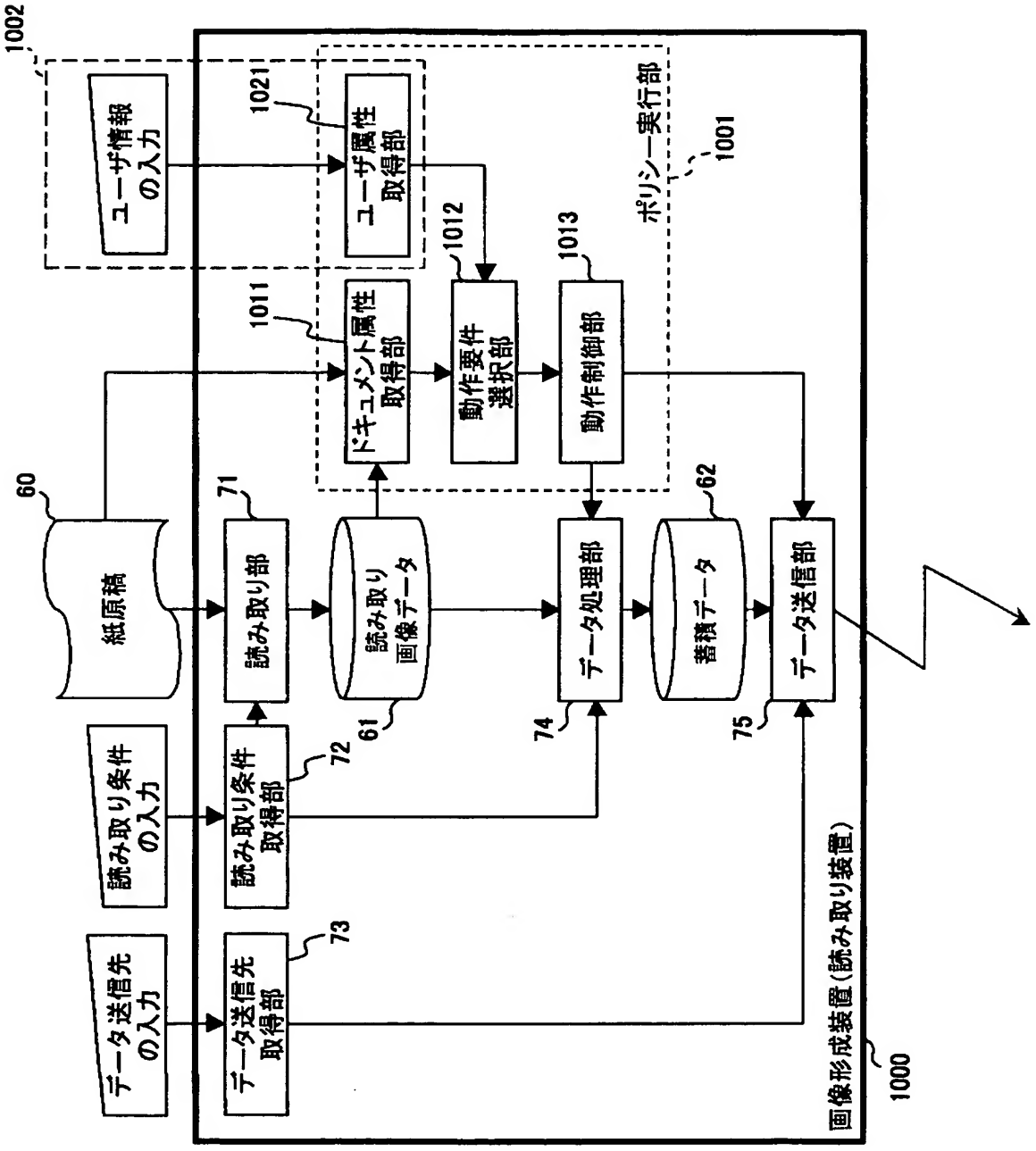
【図２７】

本発明の一実施例に係る画像形成装置の
ハードウェア構成を示すブロック図



【図２８】

セキュリティポリシーに従って動作する読み取り装置としての
画像形成装置の機能構成を示す図



【図２９】

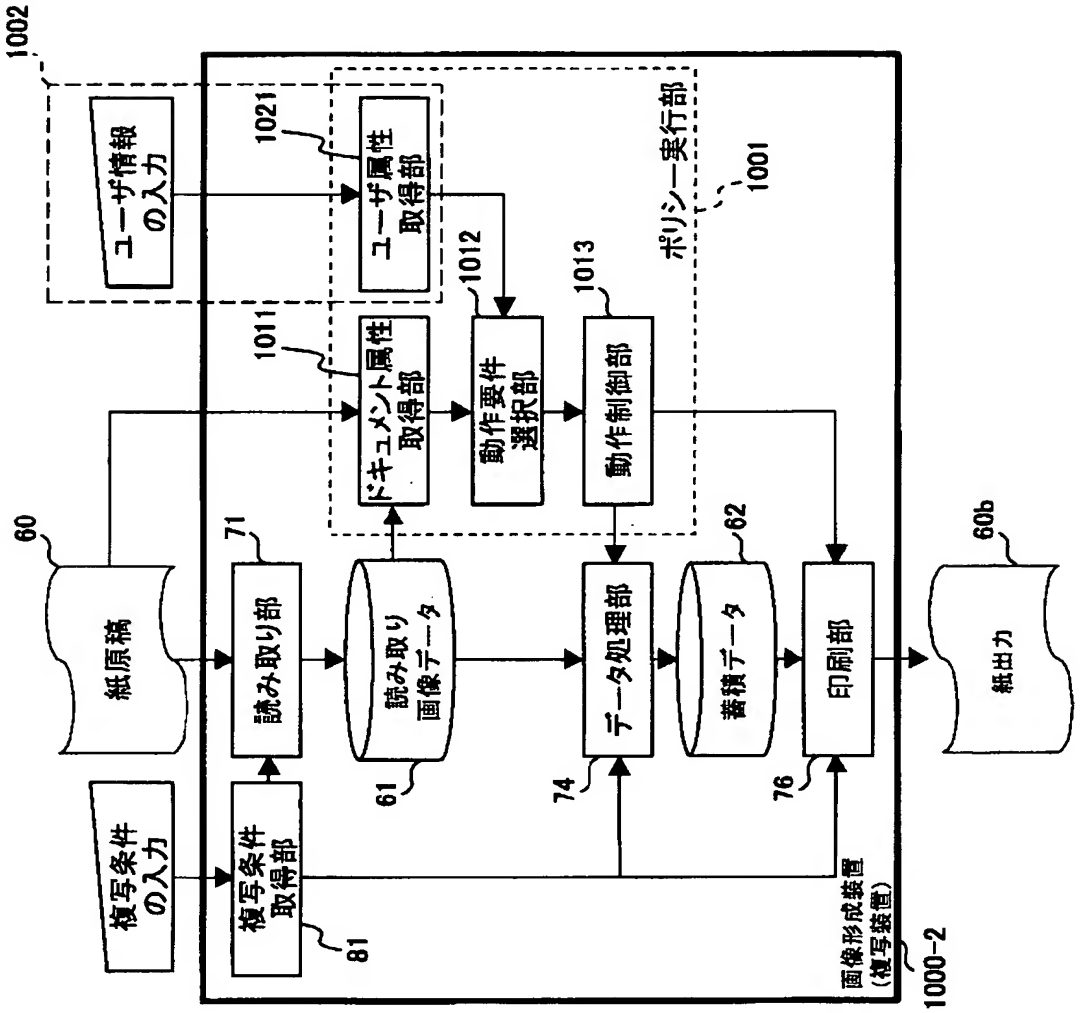
簡略化したDSPの例を示す図

2100

```
<?xml version="1.0" encoding="SHIFT-JIS" ?>
<document_security_policy>
<policy>
  <acc_rule>
    <doc_category>ANY</doc_category>
      <doc_security_level>basic</doc_security_level>
      <acl>
        <ace>
          <user_category>ANY</user_category>
          <user_security_level>ANY</user_security_level>
          <operation>
            <name>scan</name>
              <allowed/><!-- allowed without any requirement -->
            </operation>
            <operation>
              <name>net_delivery</name>
              <requirement>audit</requirement>
              <requirement>print_restriction</requirement>
              <requirement>trusted_channel</requirement>
            </operation>
          </ace>
        </acl>
      </acc_rule>
      <acc_rule>
        <doc_category>ANY</doc_category>
        <doc_security_level>high</doc_security_level>
        <acl>
          <ace>
            <user_category>DOC-CATEGORY</user_category>
            <user_security_level>ANY</user_security_level>
            <operation>
              <name>scan</name>
              <requirement>audit</requirement>
              <requirement>embed_trace_info</requirement>
            </operation>
          </ace>
        </acl>
      </acc_rule>
    </policy>
```

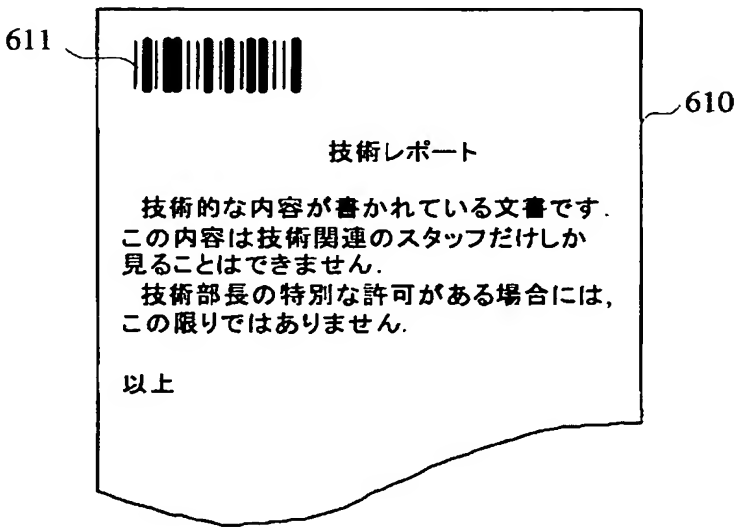
【図３０】

セキュリティポリシーに従って複写装置としての
画像形成装置の機能構成を示す図



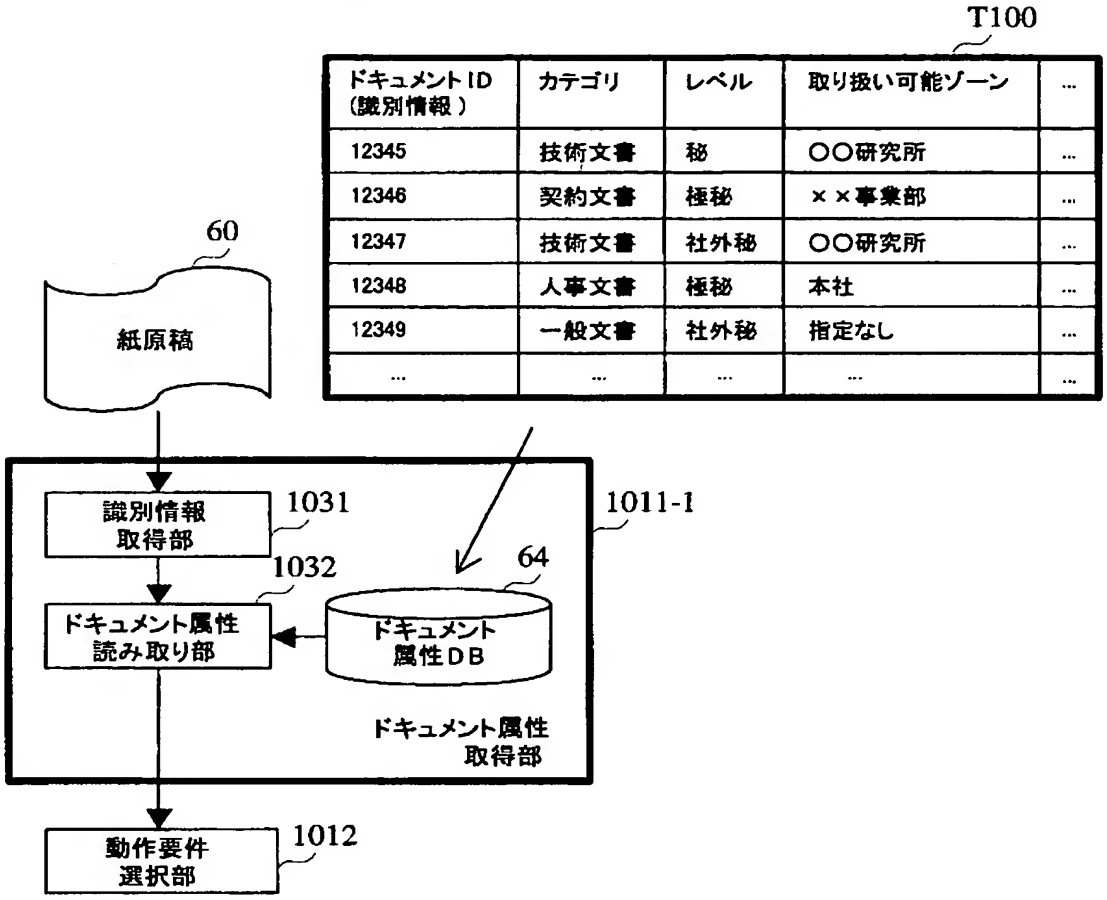
【図３１】

ドキュメントの識別情報をバーコードで印字した場合を示す図



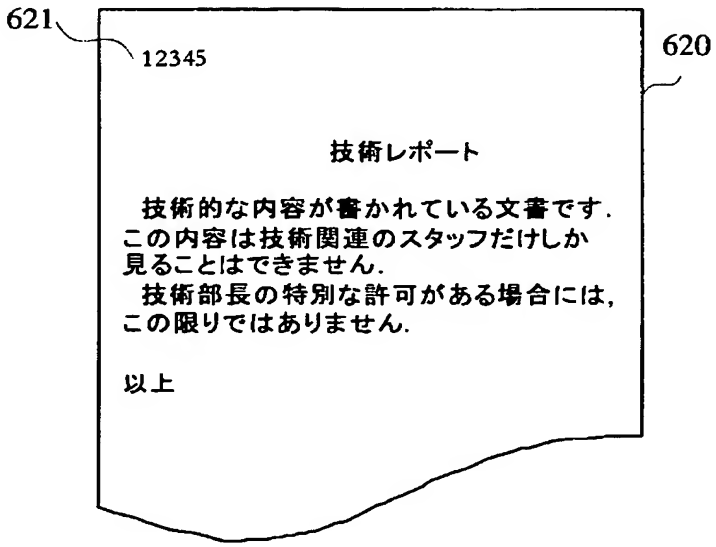
【図３２】

ドキュメント属性取得部の第1機能構成を示す図



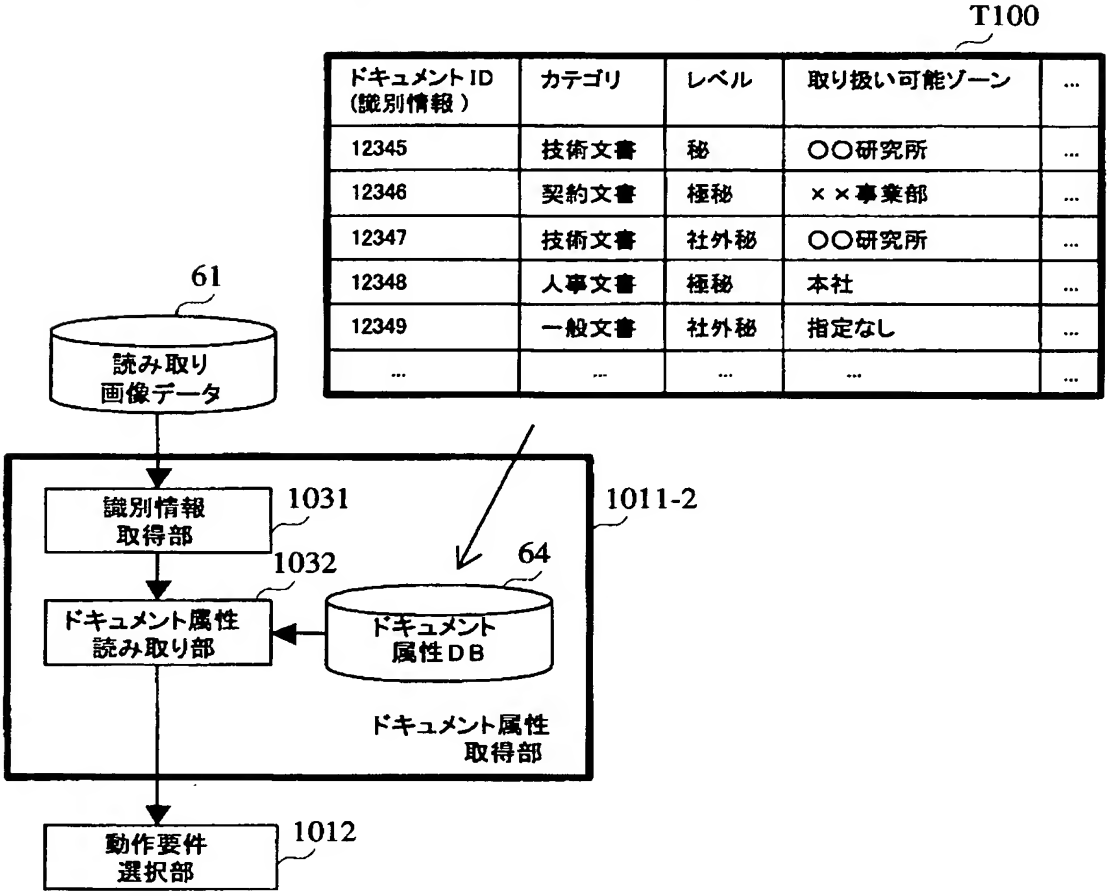
【図３３】

ドキュメントの識別情報を数字で印字した場合を示す図



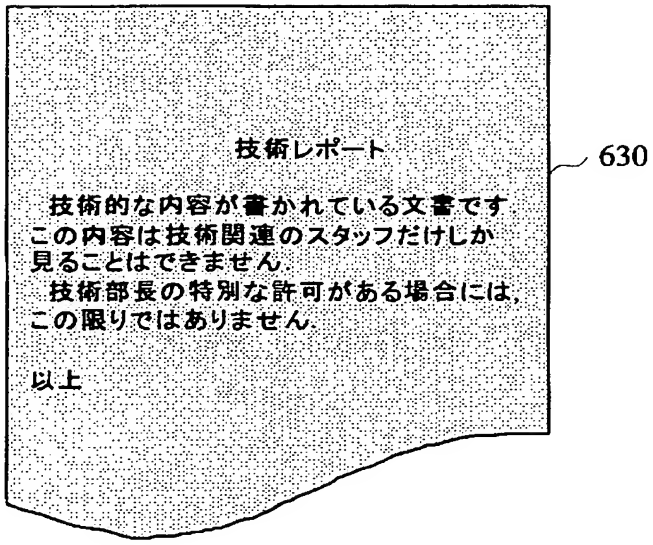
【図３４】

ドキュメント属性取得部の第2機能構成を示す図



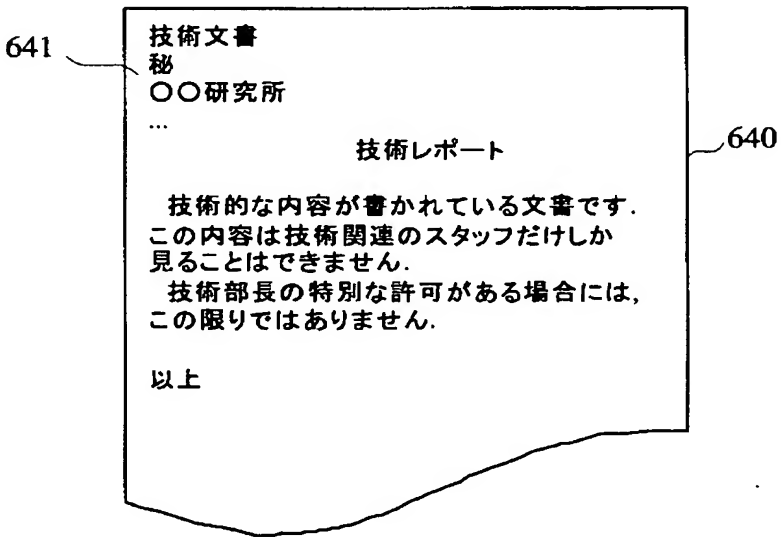
【図３５】

ドキュメントの識別情報を全面に印字した場合を示す図



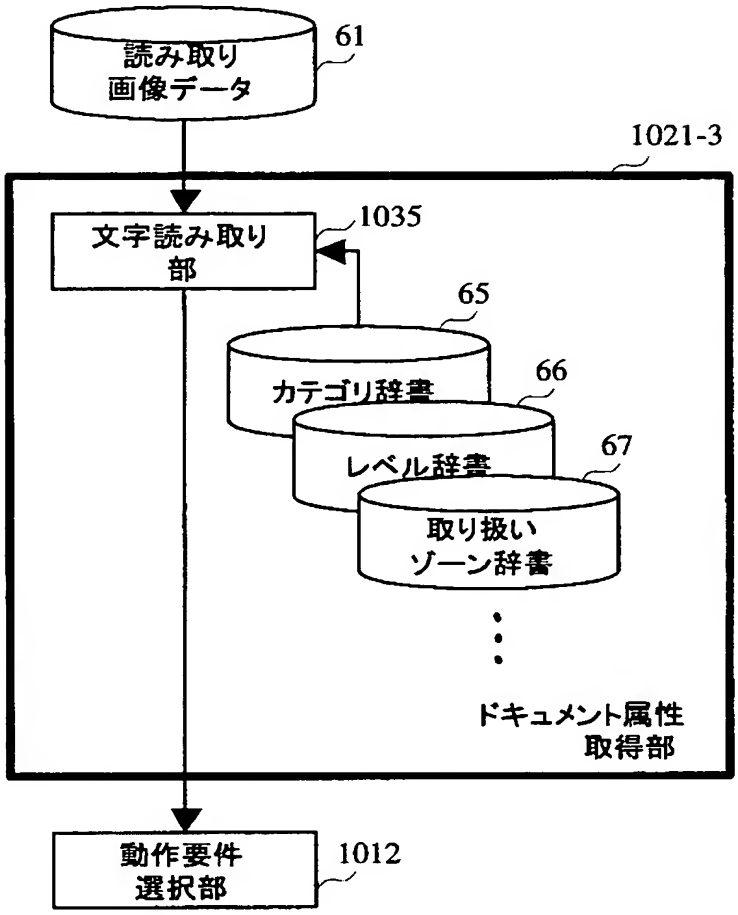

【図３６】

ドキュメントのセキュリティ属性を文字で印字した場合を示す図



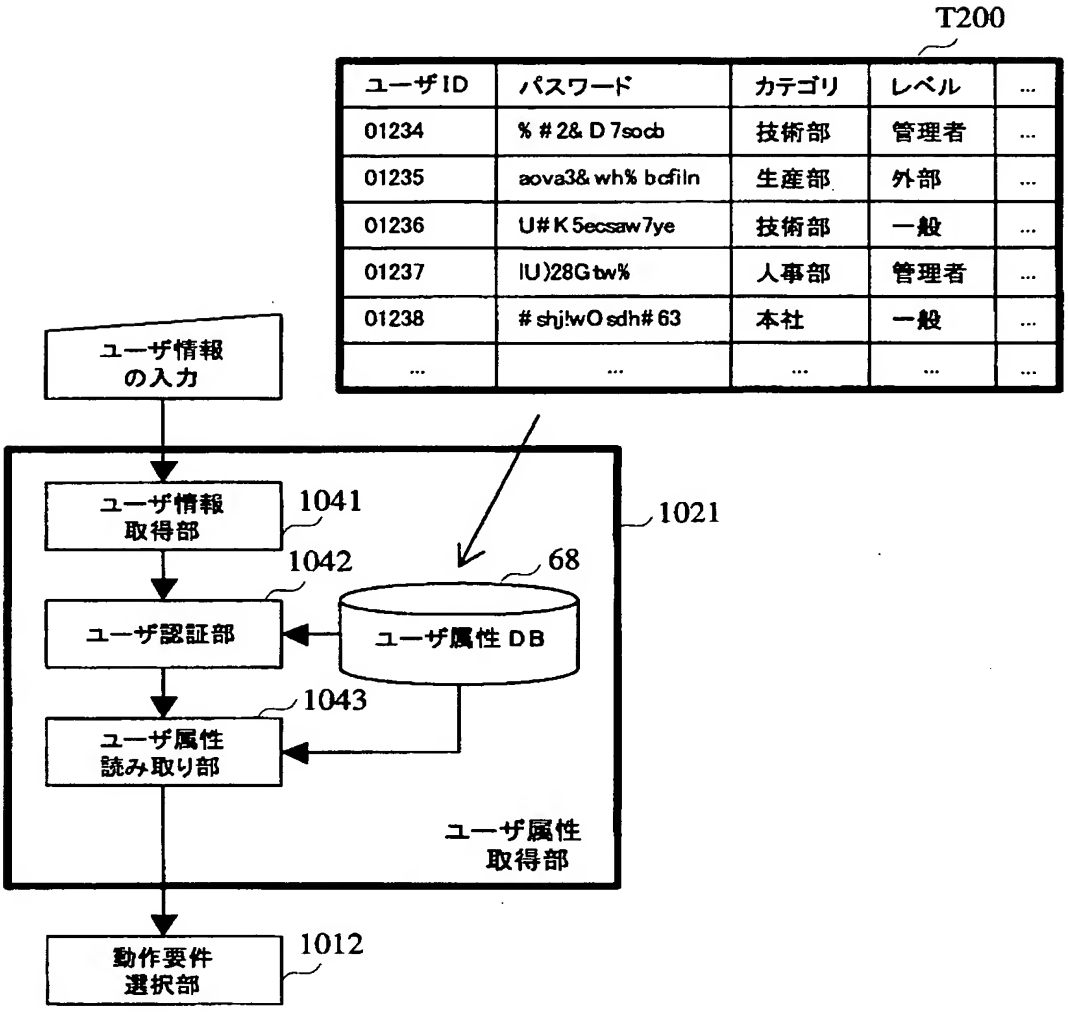
【図３７】

ドキュメント属性取得部の第3機能構成を示す図



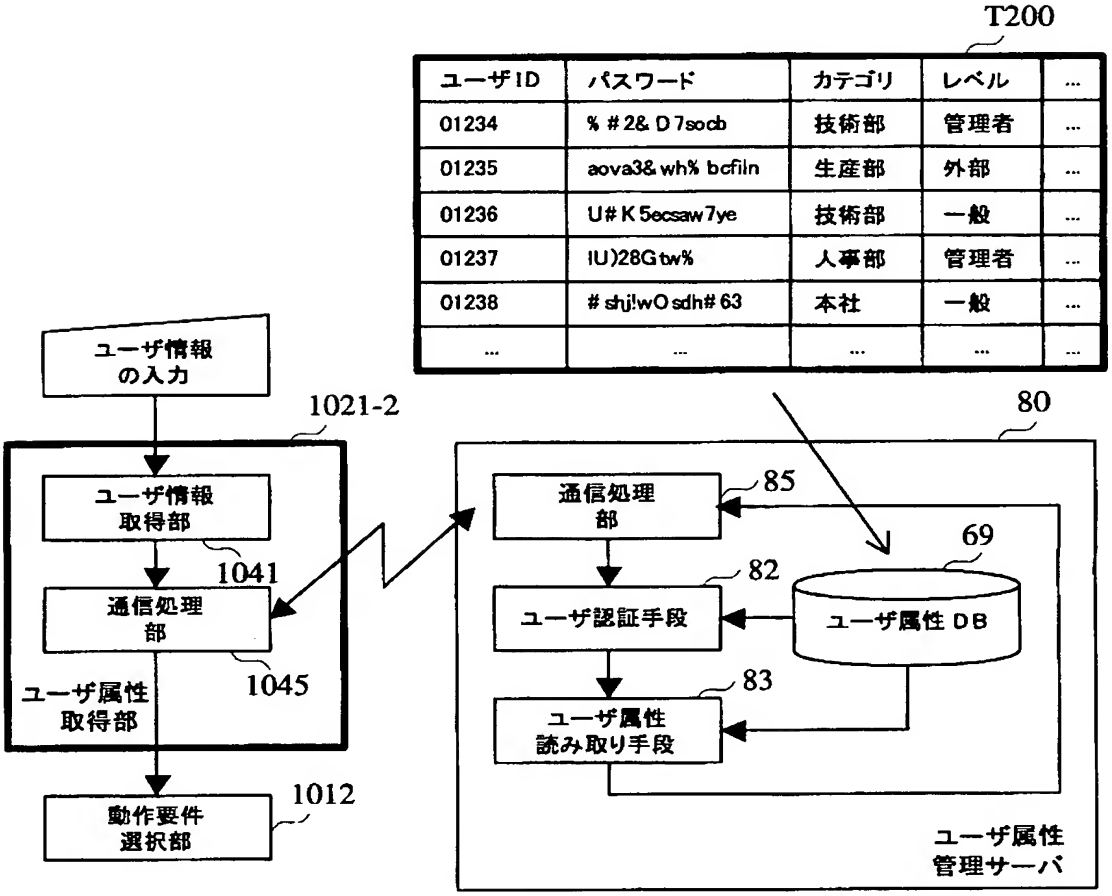
【図３８】

ユーザ属性取得部の機能構成を示す図



【図３９】

# ユーザ属性を外部サーバから取得する場合の機能構成を示す図



【書類名】要約書
【要約】
【課題】　本発明の課題は、情報システムのセキュリティを確保するシステムに関し、特に、セキュリティポリシーに基づいたドキュメントの読み取りとネットワーク配信を行う画像形成装置及び画像形成方法を提供することを目的とする。
【解決手段】　本発明の課題は、ドキュメントの識別情報を読み取る識別情報読取手段と、上記識別情報によって指定される動作要件を選択する動作要件選択手段と、上記動作要件選択手段によって選択された１つ以上の動作要件に従って所定動作の実行を制御する動作制御手段とを有する画像形成装置によって達成される。
【選択図】　図２８

特願２００３－３１４４６４

出　願　人　履　歴　情　報

識別番号　　［０００００６７４７］

１．変更年月日　　２００２年　５月１７日
［変更理由］　　住所変更
住　所　　東京都大田区中馬込１丁目３番６号
氏　名　　株式会社リコー